目　录

第二部分 解析理论

第一部分　代 数 理 论

第一章 代数数域和代数整数环

§1 代数数域

有理数域 $\mathbb{Q}$ 的有限(次)扩域 K 叫作是**代数数域**，简称作**数域**．这是代数数论的基本研究对象．如果扩张次数$[K:\mathbb{Q}]$是 n，则 K 也叫作是 n 次(数)域．由于有限扩张必然是代数扩张，所以数域 K 中每个元素均是 $\mathbb{Q}$ 上的代数元素．根据代数基本定理(附录 B，(18))，复数域 $\mathbb{C}$ 是 $\mathbb{Q}$ 的代数封闭扩域．从而数域 K 中每个元素均可看成是复数，而每个数域 K 均可看成是 $\mathbb{C}$ 的子域．如果 $K\subseteq\mathbb{R}$($\mathbb{R}$ 表示实数域)，则称 K 为**实域**，否则称 K 为**虚域**．元素 $\alpha\in\mathbb{C}$ 如果是 $\mathbb{Q}$ 上的代数元素(即存在 $f(x)\in\mathbb{Q}[x]$，$\deg f(x)\geqslant 1$，使得 $f(\alpha)=0$)，我们称 α 为**代数数**，否则便叫作是**超越数**．所有代数数全体构成域 Ω，叫作是 $\mathbb{Q}$ 的**代数闭包**．事实上每个数域均是 Ω 的子域，而 $\mathbb{C}$ 是大于 Ω 的．换句话说，超越数是存在的．例如，可以证明 π 和 e 均是超越数，并且超越数比代数数还要多(习题 1)．

关于域的代数扩张的一般事实请参见附录 B，III．在这一节里，我们就数域的情形再作一些补充．

1.1 单扩张定理

设 L/K 是数域的扩张(即 L 和 K 均是数域并且 $K\subseteq L$)．由于扩张 $L/\mathbb{Q}$ 和 $K/\mathbb{Q}$ 均是有限的，从而 L/K 也是有限扩张．令扩张次数为$[L:K]=n$，而 $\omega_1,\cdots,\omega_n$ 是向量空间 L 的一组 K-基，则 L 中每个元素均可唯一地写为

$$k_1\omega_1+\cdots+k_n\omega_n,\ k_i\in K.$$

特别地有 $L=K(\omega_1, \omega_2, \cdots, \omega_n)$，即 L/K 是有限生成扩张．我们现在要进一步证明

定理1 每个数域扩张 L/K 均是单扩张．即存在 $\gamma\in L$，使得 $L=K(\gamma)$．

证明 我们只要对 $L=K(\alpha, \beta)$ 的情形证明定理即可，因为一般情形 $L=K(\omega_1, \cdots, \omega_n)$ 可由此对 n 归纳证得．现设 $L=K(\alpha, \beta)$．令 $f(x)$，$g(x)\in K[x]$ 分别是元素 α 和 β 在 K 上的极小多项式，它们在 $\mathbb{C}[x]$ 中分解为

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i),\ g(x)=\prod_{j=1}^{m}(x-\beta_j),\ \alpha_i,\ \beta_j\in\mathbb{C}.$$

其中 $n=\deg f$, $m=\deg g$．不妨设 $\alpha=\alpha_1$，$\beta=\beta_1$．由于 $f(x)$ 和 $g(x)$ 均是 $K[x]$ 中不可约多项式，从而它们均无重根．即 α_i $(1\leqslant i\leqslant n)$ 两两相异而 $\beta_j(1\leqslant j\leqslant m)$ 也两两相异．现在于有限集合

$$\{(\alpha_i-\alpha_j)/(\beta_k-\beta_l)\,|\,1\leqslant k\neq l\leqslant m,\ 1\leqslant i\leqslant j\leqslant n\}$$

之外取一个有理数 c，不难看出 mn 个复数 $\alpha_i+c\beta_j$ 两两相异．令 $\gamma=\alpha_1+c\beta_1=\alpha+c\beta$．则多项式 $h(x)=f(\gamma-cx)$ 属于 $K(\gamma)[x]$，$h(\beta_1)=0$，而 $\beta_2, \cdots, \beta_m$ 均不为 $h(x)$ 的根．于是在 $\mathbb{C}[x]$ 中 $(h(x), g(x))=x-\beta_1$．注意域上两个多项式的最大公因子可以用辗转相除法求得，而这个过程在 $K(\gamma)[x]$ 中和 $\mathbb{C}[x]$ 中都是一样的，因此在 $K(\gamma)[x]$ 中也有 $(h(x), g(x))=x-\beta_1$．特别地 $x-\beta_1\in K(\gamma)[x]$，这就表明 $\beta=\beta_1\in K(\gamma)$，于是 $\alpha=\gamma-c\beta\in K(\gamma)$．从而 $K(\alpha, \beta)\subseteq K(\gamma)$．另一方面，由于 $\gamma=\alpha+c\beta$, $c\in K$，从而 $K(\gamma)\subseteq K(\alpha, \beta)$ 显然成立．这就证明了 $K(\alpha, \beta)=K(\gamma)$，从而也证明了定理1． ∎

1.2 数域的嵌入

设 L/K 是数域的扩张．正如附录 B, III 中所述，每个域的单同态 $\sigma: L\to\mathbb{C}$ 均叫作 L 在 $\mathbb{C}$ 中的一个嵌入．如果 σ 在 K 上的限制 $\sigma|_K$ 是域 K 上的恒等自同构(即对每个 $k\in K$ 均有 $\sigma(k)=$

k)，则称 σ 是 K-嵌入. 利用上面的单扩张定理我们可以证明：L 恰好有 $[L:K]$ 个 K-嵌入. 事实上，我们可以证明下面更为一般的结论：

定理 2 设 L/K 是数域的扩张，$[L:K]=n$. 则每个嵌入 $\sigma: K\to\mathbb{C}$ 均可以 n 种不同的方法扩充到 L 上. 换句话说，恰好存在 n 个不同的嵌入 $\tau_i: L\to\mathbb{C}(1\leqslant i\leqslant n)$，使得 $\tau_i|_K=\sigma$.

证明 由单扩张定理我们可以令 $L=K(\gamma)$. 命 $f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n\in K[x]$ 是 γ 在 K 上的极小多项式，则 $\deg f=n$，而 L 中元素均可唯一地表示成

$$\alpha=k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1},\quad k_i\in K.$$

(附录 B，(12) 及其注记). 设 $\tau: L\to\mathbb{C}$ 是一个嵌入并且 $\tau|_K=\sigma$，则 $\tau(\alpha)=\sigma(k_0)+\sigma(k_1)\tau(\gamma)+\cdots+\sigma(k_{n-1})\tau(\gamma)^{n-1}$. 从而 τ 由它在 γ 上的值所完全决定. 考虑多项式

$$\sigma f(x)=\sigma(c_0)+\sigma(c_1)x+\cdots+\sigma(c_n)x^{n-1}\in\sigma(K)[x].$$

由于 $\sigma: K\to\sigma(K)$ 是域的同构，不难看出 σf 是 $\sigma(K)[x]$ 中的 n 次不可约多项式，从而它有 n 个不同的复根 $\rho_1,\cdots,\rho_n$. 由于 $\sigma f(\tau(\gamma))=\sigma(c_0)+\sigma(c_1)\tau(\gamma)+\cdots+\sigma(c_{n-1})\tau(\gamma)^{n-1}=\tau(f(\gamma))=0$，这就表明 $\tau(\gamma)$ 必为某个 ρ_i. 从而 σ 到 L 上的扩充至多有 n 个. 现在对每个 $i(1\leqslant i\leqslant n)$，作映射

$$\tau_i: L\to\mathbb{C},\quad \tau_i(k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1})=\sigma(k_0)+\sigma(k_1)\rho_i+\cdots+\sigma(k_{n-1})\rho_i^{n-1},$$

易验证这是域的同态. 设 $k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1}\in\operatorname{Ker}\tau_i$ (同态 τ_i 的核)，则 $\sigma(k_0)+\sigma(k_1)\rho_i+\cdots+\sigma(k_{n-1})\rho_i^{n-1}=0$，从而

$$\sigma f(x)\,|\,\sigma(k_0)+\sigma(k_1)x+\cdots+\sigma(k_{n-1})x^{n-1},$$

于是 $f(x)\,|\,k_0+k_1x+\cdots+k_{n-1}x^{n-1}$ (为什么?). 但是 $f(x)$ 为 $K[x]$ 中 n 次不可约多项式，所以只能是 $k_0=k_1=\cdots=k_{n-1}=0$. 这就表明 $\operatorname{Ker}\tau_i=(0)$，即 τ_i 是嵌入. 又显然 $\tau_i|_K=\sigma$ 并且 $\tau_i(\gamma)=\rho_i$. 而 $\rho_i(1\leqslant i\leqslant n)$ 是两两相异的，从而 $\tau_i(1\leqslant i\leqslant n)$ 是 σ 到 L 上的 n 个不同的扩充. 这就证明了定理 2. ∎

在定理 2 中特别取 σ 为域 K 的恒等自同构，我们就得到：

系 每个数域扩张 L/K 均恰好有 $[L:K]$ 个从 L 到 $\mathbb{C}$ 的 K-嵌入.

设 $L=K(\gamma)$, $f(x)\in K[x]$ 是 γ 在 K 上的极小多项式. $\deg f=n=[L:K]$. 令 $\gamma_i(1\leqslant i\leqslant n)$ 是 f 的 n 个不同的根(其中有一个为 γ), 它们即是 γ 的全部 K-共轭元素(附录 B, III). 根据定理 2 的证明, 可知 τ_i: $L=K(\gamma)\xrightarrow{\sim}K(\gamma_i)\subseteq\mathbb{C}$, $\tau_i(\gamma)=\gamma_i$ $(1\leqslant i\leqslant n)$ 就是 L 的全部 n 个嵌入, 从而 $K(\gamma_i)$ $(1\leqslant i\leqslant n)$(它们不必不同)就是 L 的全部 K-共轭域. 当 $K(\gamma_i)=L(1\leqslant i\leqslant n)$ 即 L 为 K-自共轭域的时候, L/K 即为**伽罗华扩张**(或者叫**正规扩张**). 这也等价于说: $\gamma_i\in L(1\leqslant i\leqslant n)$. 这时, 每个 K-嵌入 τ_i: $L\to\mathbb{C}$ 均是域 L 的 K-自同构. 从而伽罗华群 $\mathrm{Gal}(L/K)=\{\tau_1,\tau_2,\cdots,\tau_n\}$. 而对于一般的情形, 由于 $K(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 是 $f(x)$ 在 K 上的分裂域, 从而 $K(\gamma_1,\cdots,\gamma_n)/K$ 是伽罗华扩张(附录 B, III, (15)). 并且不难看出 $K(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 是 K 的包含 L 的最小伽罗华扩张. 称 $K(\gamma_1,\cdots,\gamma_n)$ 为扩张 L/K 的**正规闭包**.

如果 $K=\mathbb{Q}$, 即 L 是 $n=[L:\mathbb{Q}]$ 次数域, $L=\mathbb{R}(\gamma)$. 令 $f(x)\in\mathbb{Q}[x]$ 是 γ 在 $\mathbb{Q}$ 上的极小多项式, 则存在恰好 n 个域的嵌入 τ_i: $L=\mathbb{Q}(\gamma)\xrightarrow{\sim}\mathbb{Q}(\gamma_i)\subseteq\mathbb{C}$, 使得 $\tau_i(\gamma)=\gamma_i(1\leqslant i\leqslant n)$, 其中 $\gamma_i(1\leqslant i\leqslant n)$ 是 $f(x)$ 的 n 个不同的根(注意: 数域的嵌入必为 $\mathbb{Q}$-嵌入!). 不妨设前 r_1 个是实根而后 r_2 对是虚根, 即

$$\gamma_1\in\mathbb{R}\quad(1\leqslant i\leqslant r_1),$$

$$\gamma_{r_1+j}=\overline{\gamma}_{r_1+r_2+j}\notin\mathbb{R}\quad(1\leqslant j\leqslant r_2,\ r_1+2r_2=n).$$

于是 L 的前 r_1 个共轭域 $\mathbb{Q}(\gamma_i)$ 为实域, 我们称这 r_1 个嵌入 τ_i: $L=\mathbb{R}(\gamma)\xrightarrow{\sim}\mathbb{Q}(\gamma_i)\subseteq\mathbb{R}$ 为**实嵌入**. 而后 r_2 对共轭域为虚域, 并且 $\mathbb{Q}(\gamma_{r_1+j})=\mathbb{Q}(\gamma_{r_1+r_2+j})\not\subset\mathbb{R}(1\leqslant j\leqslant r_2)$. 称这 r_2 对嵌入 $\tau_i(r_1+1\leqslant i\leqslant n)$ 为**复嵌入**, 并且称 τ_{r_1+j} 和 $\tau_{r_1+r_2+j}$ 是彼此共轭的嵌入, 记为 $\overline{\tau}_{r_1+j}=\tau_{r_1+r_2+j}(1\leqslant j\leqslant r_2)$.

例 1 每个二次(数)域均可唯一地表示成 $\mathbb{Q}(\sqrt{d})$, 其中 d 为无平方因子整数(习题 2). 当 $d>0$ 时这是实域称作是实二次域. 而当 $d<0$ 时 $\mathbb{Q}(\sqrt{d})$ 是虚域, 称作是虚二次域. 由于

$\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 必然是伽罗华扩张，可知对于实二次域 $r_1=2$，$r_2=0$，而对于虚二次域 $r_1=0$，$r_2=1$. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 的伽罗华群为 $G=\{I, \sigma\}$，其中 I 表示恒等自同构，而 $\sigma(a+b\sqrt{d})=a-b\sqrt{d}$ $(a, b\in\mathbb{Q})$，即将 $\mathbb{Q}(\sqrt{d})$ 中每个元素 $a+b\sqrt{d}$ 映成它的共轭元素 $a-b\sqrt{d}$. 有时也将 σ 称作是二次域 $\mathbb{Q}(\sqrt{d})$ 的共轭自同构.

例 2 分圆域 $\mathbb{Q}(\zeta_{p^n})$，其中 $\zeta_{p^n}=e^{2\pi i/p^n}$ 是 p^n 次本原单位根，而 p 为素数，$n\geqslant 1$. 以下简记 $\zeta=\zeta_{p^n}$. 易知 ζ 是多项式

$$\begin{aligned}f(x)&=x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+x^{p^{n-1}}+1\\&=(x^{p^n}-1)/(x^{p^{n-1}}-1)\in\mathbb{Z}[x]\end{aligned}$$

的根. 我们现在证明 $f(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式. 为此令 $g(x)=f(x+1)=x^{(p-1)p^{n-1}}+c_{p^n-p^{n-1}-1}x^{p^n-p^{n-1}-1}+\cdots+c_1x+c_0\in\mathbb{Z}[x]$. 由于

$$g(x)=\frac{(x+1)^{p^n}-1}{(x+1)^{p^{n-1}}-1}\equiv\frac{x^{p^n}}{x^{p^{n-1}}}=x^{p^n-p^{n-1}}\quad(\bmod p),$$

从而 $p\mid c_i$ $(0\leqslant i\leqslant p^n-p^{n-1}-1)$. 进而 $c_0=g(0)=f(1)=p$，于是 $p^2\nmid c_0$. 所以由 Eisenstein 判别准则(附录 B, (7))可知 $g(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式，从而 $f(x)$ 也是如此. 这就表明 $f(x)$ 是 ζ 在 $\mathbb{Q}$ 上的极小多项式. 并且 $[\mathbb{Q}(\zeta_{p^n}):\mathbb{Q}]=\deg f=p^n-p^{n-1}$. ζ 的全部共轭元素(即 $f(x)$ 的全部根)显然是 ζ^i $(1\leqslant i\leqslant p^n,\ p\nmid i)$ (即为 $x^{p^n}-1$ 之根但不为 $x^{p^{n-1}}-1$ 之根者)，它们均属于 $\mathbb{Q}(\zeta)$，从而 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是伽罗华扩张. 令 $\sigma_i\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$，使得 $\sigma_i(\zeta)=\zeta^i$ $(1\leqslant i\leqslant p^n-1,\ p\nmid i)$，则

$$\sigma_i\cdot\sigma_j(\zeta)=\sigma_i(\zeta^j)=\sigma_i(\zeta)^j=\zeta^{ij}=\sigma_{ij}(\zeta).$$

这就表明 $\sigma_i\cdot\sigma_j=\sigma_{ij}$. 作映射

$$\chi:\ \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\to(\mathbb{Z}/p^n\mathbb{Z})^\times,\ \chi(\sigma_i)=\bar{i},$$

其中 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 表示环 $\mathbb{Z}/p^n\mathbb{Z}$ 的单位(乘法)群，而 $\bar{i}$ 表示剩余类 $i(\bmod p^n)$. 由上述不难看出 χ 是群的同构. 但是当 $p\geqslant 3$ 时，从初等数论我们知道，乘法群 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 是由模 p^n 的某个原根 g 生成的 p^n-p^{n-1} 阶循环群. 从而伽罗华群 $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ 当 $p\geqslant 3$ 时是 p^n-p^{n-1} 阶循环群，生成元为 σ_g.

当 $p^n\geqslant 3$ 时，$\zeta_{p^n}^i\ (1\leqslant i\leqslant p^n,\ p\nmid i)$ 均不为实数．从而对于分圆域 $\mathbb{Q}(\zeta_{p^n})\ (p^n\geqslant 3)$ 我们有 $r_1=0$，$r_2=\frac{1}{2}(p^n-p^{n-1})$．

例 3 纯三次域 $\mathbb{Q}(\sqrt[3]{2})$．元素 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^3-2．于是 $\sqrt[3]{2}$ 的共轭元素为 $\sqrt[3]{2}$，$\sqrt[3]{2}\,\omega$ 和 $\sqrt[3]{2}\,\omega^2$，其中 $\omega=\zeta_3$．由此可见 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是伽罗华扩张，其正规闭包为 $M=\mathbb{Q}(\sqrt[3]{2},\ \sqrt[3]{2}\,\omega,\ \sqrt[3]{2}\,\omega^2)=\mathbb{Q}(\sqrt[3]{2},\ \omega)$．不难算出 $[M:\mathbb{Q}]=6$ 而 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$．并且对于域 $\mathbb{Q}(\sqrt[3]{2})$ 有 $r_1=r_2=1$．

1.3 范与迹

设 L/K 为数域扩张，$[L:K]=n$．σ_i: $L\rightarrow\mathbb{C}\ (1\leqslant i\leqslant n)$ 是 L 的 n 个 K-嵌入．对于 $\alpha\in L$ 定义

$$N_{L/K}(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha),\quad T_{L/K}(\alpha)=\sum_{i=1}^{n}\sigma_i(\alpha).$$

分别称作是元素 $\alpha\in L$ 对于扩张 L/K 的范和迹．从定义可知 $N_{L/K}$ 和 $T_{L/K}$ 有如下简单性质：

(a) 对于 $\alpha,\beta\in L$，$N_{L/K}(\alpha\beta)=N_{L/K}(\alpha)N_{L/K}(\beta)$，$T_{L/K}(\alpha+\beta)=T_{L/K}(\alpha)+T_{L/K}(\beta)$；

(b) 对于 $\alpha\in K$，$N_{L/K}(\alpha)=\alpha^n$，$T_{L/K}(\alpha)=n\alpha$，其中 $n=[L:K]$．

下面定理 3 给出范和迹的一种计算方法．

定理 3 设 L/K 为数域扩张，$[L:K]=n$．$\alpha\in L$，$f(x)=x^m-c_1x^{m-1}+\cdots+(-1)^m c_m\in K[x]$ 是 α 在 K 上的极小多项式，$m=[K(\alpha):K]$，则

$$N_{L/K}(\alpha)=c_m^{n/m},\ T_{L/K}(\alpha)=\frac{n}{m}c_1.$$

证明 设 $\alpha_1=\alpha,\ \alpha_2,\ \cdots,\ \alpha_m$ 是 $f(x)$ 的 m 个根．由定义知

$$T_{K(\alpha)/K}(\alpha)=\alpha_1+\alpha_2+\cdots+\alpha_m=c_1,$$
$$N_{K(\alpha)/K}(\alpha)=\alpha_1\alpha_2\cdots\alpha_m=c_m.$$

根据定理 2，每个 K-嵌入 τ_i: $K(\alpha)\rightarrow\mathbb{C}\ (\tau_i(\alpha)=\alpha_i)$ 均可扩充成 $[L:K(\alpha)]=n/m$ 个嵌入 σ_{ij}: $L\rightarrow\mathbb{C}\ (1\leqslant j\leqslant n/m)$．不难看出

$\{\sigma_{ij} | 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n/m\}$是彼此不同的，从而构成 L 到 $\mathbb{C}$ 的全部 K-嵌入。于是

$$N_{L/K}(\alpha)=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\sigma_{ij}(\alpha)=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\tau_i(\alpha)=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\alpha_i$$
$$=(\alpha_1\cdots\alpha_m)^{n/m}=c_n^{n/m},$$
$$T_{L/K}(\alpha)=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\sigma_{ij}(\alpha)=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\tau_i(\alpha)=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\alpha_i$$
$$=n/m(\alpha_1+\cdots+\alpha_m)=\frac{n}{m}c_1. \quad \blacksquare$$

注记 从定理3特别得到，对于每个 $\alpha\in L$，$N_{L/K}(\alpha)$ 和 $T_{L/K}(\alpha)$都是 K 中的元素。再由性质(a)和(b)可知 $T_{L/K}$: $L\to K$ 是加法群同态，而 $N_{L/K}$: $L^\times\to K^\times$ 是乘法群同态，这里 $L^\times=L-\{0\}$.

定理4(传递公式) 设 L/M，M/K 均是数域扩张，$\alpha\in L$，则

$$N_{L/K}(\alpha)=N_{M/K}(N_{L/M}(\alpha)),\ T_{L/K}(\alpha)=T_{M/K}(T_{L/M}(\alpha)).$$

证明 令 $n=[L:M]$，$m=[M:K]$. $\sigma_1,\ \cdots,\ \sigma_n$ 为 L 到 $\mathbb{C}$ 中 n 个不同的 M-嵌入，$\tau_1,\ \cdots,\ \tau_m$ 为 M 到 $\mathbb{C}$ 中 m 个不同的 K-嵌入。取 S 为扩张 L/K 的正规闭包。令 $\tilde{\sigma}_i$, $\tilde{\tau}_j$ 分别为 σ_i 和 τ_j 到 S 上的一个扩充(定理2)，它们都是伽罗华群 $\mathrm{Gal}(S/K)$ 中的元素。从而$(\tilde{\tau}_j\tilde{\sigma}_i)|_L(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m)$均是 L 到 $\mathbb{C}$ 中的 K-嵌入。我们现在证明这 nm 个 K-嵌入彼此不同：如果 $j\neq j'$，则存在 $b\in M$，使得 $\tau_j(b)\neq\tau_{j'}(b)$. 于是

$$(\tilde{\tau}_j\tilde{\sigma}_i)|_L(b)=\tilde{\tau}_j\tilde{\sigma}_i(b)=\tilde{\tau}_j\tilde{\sigma}_i(b)=\tilde{\tau}_j(b)$$
$$=\tau_j(b)\neq\tau_{j'}(b)=(\tilde{\tau}_{j'}\tilde{\sigma}_{i'})|_L(b).$$

这就表明当 $j\neq j'$ 时 $(\tilde{\tau}_j\tilde{\sigma}_i)|_L\neq(\tilde{\tau}_{j'}\tilde{\sigma}_{i'})|_L$. 如果 $j=j'$ 但是 $i\neq i'$，则存在 $c\in L$，使得 $\sigma_i(c)\neq\sigma_{i'}(c)$. 于是

$$(\tilde{\tau}_j\tilde{\sigma}_i)|_L(c)=\tilde{\tau}_j(\sigma_i(c))\neq\tilde{\tau}_j(\sigma_{i'}(c))=(\tilde{\tau}_j\tilde{\sigma}_{i'})|_L(c).$$

从而当 $i\neq i'$ 时，$(\tilde{\tau}_j\tilde{\sigma}_i)|_L\neq(\tilde{\tau}_j\tilde{\sigma}_{i'})|_L$. 因此$(\tilde{\tau}_j\tilde{\sigma}_i)|_L(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m)$就是 L 到 $\mathbb{C}$ 中的全部 $nm=[L:K]$个 K-嵌入。从而对于每个 $\alpha\in L$，

$$N_{L/K}(\alpha)=\prod_{1\leq j\leq m}\prod_{1\leq i\leq n}(\tilde{\tau}_j\tilde{\sigma}_i)\big|_L(\alpha)=\prod_{j=1}^{m}\tilde{\tau}_j\Big(\prod_{i=1}^{n}\tilde{\sigma}_i(\alpha)\Big)$$

$$=\prod_{j=1}^{m}\tilde{\tau}_j(N_{L/M}(\alpha))=N_{M/K}(N_{L/M}(\alpha)).$$

对于迹可以类似地证明. ∎

1.4 元素的判别式

设 L/K 是数域的 n 次扩张, $\sigma_1, \cdots, \sigma_n$ 是 L 到 $\mathbb{C}$ 的 n 个 K-嵌入. $\alpha_1, \cdots, \alpha_n$ 为 L 中任意 n 个元素. 定义

$$d_{L/K}(\alpha_1, \cdots, \alpha_n)=\left|\left(\sigma_i(\alpha_j)\right)_{\substack{1\leq i\leq n\\1\leq j\leq n}}\right|^2$$

($|\ |$表示方阵的行列式), 称作是元素$\{\alpha_1, \cdots, \alpha_n\}$对于扩张 L/K 的判别式(从定义不难看出, 这个判别式与元素 $\alpha_1, \cdots, \alpha_n$ 的次序是无关的). 下面引理表明它是 K 中的元素.

引理 1 $d_{L/K}(\alpha_1, \cdots, \alpha_n)=|(T_{L/K}(\alpha_i\alpha_j))|$

证明

$$左边=\begin{vmatrix}\sigma_1(\alpha_1), & \cdots, & \sigma_n(\alpha_1)\\ & \cdots\cdots & \\ \sigma_1(\alpha_n), & \cdots, & \sigma_n(\alpha_n)\end{vmatrix}\begin{vmatrix}\sigma_1(\alpha_1), & \cdots, & \sigma_1(\alpha_n)\\ & \cdots\cdots & \\ \sigma_n(\alpha_1), & \cdots, & \sigma_n(\alpha_n)\end{vmatrix}$$

$$=\left|\left(\sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j)\right)\right|=右边. \quad ∎$$

判别式的第一个应用是它可用来判别 L 中 n 个元素 $\alpha_1, \cdots, \alpha_n$ 是否为向量空间 L 的一组 K-基.

引理 2 $d_{L/K}(\alpha_1, \cdots, \alpha_n)\neq 0\Leftrightarrow\alpha_1, \cdots, \alpha_n$ 是 K-线性无关的.

证明 $\Rightarrow$: 如果 $\alpha_1, \cdots, \alpha_n$ 是 K-线性相关的, 即存在不全为零的 $k_1, \cdots, k_n\in K$, 使得 $k_1\alpha_1+\cdots+k_n\alpha_n=0$. 于是

$$k_1\sigma_i(\alpha_1)+\cdots+k_n\sigma_i(\alpha_n)=\sigma_i(k_1\alpha_1+\cdots+k_n\alpha_n)=0 \quad (1\leq i\leq n).$$

这表明 n 阶方阵$(\sigma_i(\alpha_j))$的诸列是 K-线性相关的. 从而 $d_{L/K}(\alpha_1, \cdots, \alpha_n)=|(\sigma_i(\alpha_j))|^2=0$.

$\Leftarrow$: 如果 $d_{L/K}(\alpha_1, \cdots, \alpha_n)=0$, 则 $|(T_{L/K}(\alpha_i\alpha_j))|=0$ (引理 1), 从而方阵$(T_{L/K}(\alpha_i\alpha_j))$的 n 个行 $R_1, \cdots, R_n$ 是 K-线性相关的, 其中 $R_i=(T_{L/K}(\alpha_i\alpha_1), \cdots, T_{L/K}(\alpha_i\alpha_n))(1\leq i\leq n)$. 于是有不

全为零的 $k_1, \cdots, k_n\in K$，使得 $k_1R_1+\cdots+k_nR_n=0$. 如果 $\alpha_1, \cdots, \alpha_n$ 是 K-线性无关的，则 $\alpha=k_1\alpha_1+\cdots+k_n\alpha_n\neq 0$，而 $T_{L/K}(\alpha\alpha_j)=0$，因为它是向量 $k_1R_1+\cdots+k_nR_n=0$ 中的第 j 个元素 $(1\leqslant j\leqslant n)$. 由于当 $\alpha_1, \cdots, \alpha_n$ K-线性无关时，它们形成向量空间 L 的一组 K-基. 因此对于任何 $\beta\in L$ 均有 $T_{L/K}(\alpha\beta)=0$. 特别取 $\beta=\alpha^{-1}$(注意 $\alpha\neq 0$)，则我们有 $0=T_{L/K}(\alpha\alpha^{-1})=T_{L/K}(1)=[L:K]\neq 0$. 这一矛盾表明 $\alpha_1, \cdots, \alpha_n$ 是 K-线性相关的. ∎

引理 3 设 $L=K(\alpha)$, $[L:K]=n$, $f(x)$ 是 α 在 K 上的极小多项式，$\alpha_1=\alpha, \alpha_2, \cdots, \alpha_n$ 为 $f(x)$ 的 n 个复根，则

$$d_{L/K}(1, \alpha, \cdots, \alpha^{n-1})=\prod_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2$$
$$=(-1)^{\frac{n(n-1)}{2}}N_{L/K}(f'(\alpha)).$$

证明 上式左边 $=\left|(\sigma_i(\alpha^j))_{\substack{1\leqslant i\leqslant n\\0\leqslant j\leqslant n-1}}\right|^2=\left|(\alpha_i^j)_{\substack{1\leqslant i\leqslant n\\0\leqslant j\leqslant n-1}}\right|^2$.

而后一行列式是 Vandermonde 行列式. 从而可知原式左边等于 $\prod\limits_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2$. 进而，$(\alpha_r-\alpha_s)^2=-(\alpha_r-\alpha_s)(\alpha_s-\alpha_r)$，而满足 $1\leqslant r<s\leqslant n$ 的 (r, s) 共有 $\frac{1}{2}n(n-1)$ 对. 于是

$$\prod_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2=(-1)^{n(n-1)/2}\prod_{1\leqslant r\neq s\leqslant n}(\alpha_r-\alpha_s)$$
$$=(-1)^{n(n-1)/2}\prod_{r=1}^{n}\prod_{\substack{s=1\\s\neq r}}^{n}(\alpha_r-\alpha_s).$$

但是 $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$，从而 $f'(\alpha_r)=\prod\limits_{\substack{s=1\\s\neq r}}^{n}(\alpha_r-\alpha_s)$. 于是

$$\prod_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2=(-1)^{n(n-1)/2}\prod_{r=1}^{n}f'(\alpha_r)$$
$$=(-1)^{n(n-1)/2}N_{L/K}f'(\alpha).$$

注记 对于 L 中任意元素 α，令 $d_{L/K}(\alpha)=d_{L/K}(1, \alpha, \cdots, \alpha^{n-1})$，$n=[L:K]$，称作是 L 中元素 α 对于扩张 L/K 的判别式. 从引理 2 和引理 3 不难看出：$d_{L/K}(\alpha)\neq 0\Leftrightarrow 1, \alpha, \cdots, \alpha^{n-1}$ 是 K-线性无关的 $\Leftrightarrow L=K(\alpha)$. 当 $K=\mathbb{Q}$ 时，我们把 $d_{L/\mathbb{Q}}(\alpha)$ 也简写作 $d_L(\alpha)$.

例 考虑分圆域 $L=\mathbb{Q}(\omega)$, $\omega=e^{2\pi i/p^n}$, p 为奇素数, $n\geqslant 1$. 令 $s=p^n-p^{n-1}$, 我们已经知道 L 是 s 次域, ω 在 $\mathbb{Q}$ 上的极小多项式为 $f(x)=(x^{p^n}-1)/(x^{p^{n-1}}-1)=x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+x^{p^{n-1}}+1$. 于是

$$(x^{p^{n-1}}-1)f(x)=x^{p^n}-1,$$

$$(x^{p^{n-1}}-1)f'(x)+p^{n-1}x^{p^{n-1}-1}f(x)=p^n x^{p^n-1}.$$

因此 $f'(\omega)=p^n/(\omega(\omega^{p^{n-1}}-1))$. 于是由引理 3 可知

$$d_L(\omega)=(-1)^{s(s-1)/2}N(p^n)/(N(\omega)N(\omega^{p^{n-1}}-1))$$

其中 $N=N_{L/\mathbb{Q}}$. 易知 $N(p^n)=p^{ns}$, $N(\omega)=\prod_{\substack{k=1\\ p\nmid k}}^{p^n-1}\omega^k=\prod_{\substack{k=1\\ p\nmid k}}^{(p^n-1)/2}(\omega^k\cdot\omega^{-k})=1$. 剩下只需计算 $N(\omega^{p^{n-1}}-1)$. 令 $\zeta=\omega^{p^{n-1}}=e^{2\pi i/p}$, 则 ζ 在 $\mathbb{Q}$ 上的极小多项式为 $g(x)=x^{p-1}+x^{p-2}+\cdots+x+1$, 从而 $\zeta-1$ 在 $\mathbb{Q}$ 上的极小多项式为 $g(x+1)=x^{p-1}+\cdots+p$. 令 $M=\mathbb{Q}(\zeta)$, 则 $[M:\mathbb{Q}]=p-1$, 于是 $[L:M]=s/(p-1)=p^{n-1}$. 从而

$$\begin{aligned}N_{L/\mathbb{Q}}(\zeta-1)&=N_{M/\mathbb{Q}}(N_{L/M}(\zeta-1))=N_{M/\mathbb{Q}}(\zeta-1)^{p^{n-1}}\\&=p^{p^{n-1}}(-1)^{p-1}=p^{p^{n-1}}.\end{aligned}$$

从而最后得到

$$d_L(\omega)=(-1)^{s(s-1)/2}p^{ns}/p^{p^{n-1}}=(-1)^{s(s-1)/2}p^{p^{n-1}(np-n-1)}.$$

请读者验证, 当 $p=2$ 时这个公式仍然成立.

1.5 单位根

数域 K 中的乘法有限阶元素 $w\neq 0$ 叫作是 K 中的**单位根**. 如果 $w^n=1$, 则称 w 为 n 次单位根. 如果 w 的乘法阶数恰好是 n, 即 n 是满足 $w^n=1$ 的最小正整数, 则称 w 是 n 次本原单位根. 数域 K 中的单位根全体 W_K 显然形成乘法群, 称作是数域 K 的**单位根群**. 我们现在要证明 W_K 是有限循环群. 首先证明

引理 4 W_K 是有限群.

证明 设 w 是数域 K 中的 n 次单位根. 令 $f(x)=x^m+c_1x^{m-1}+\cdots+c_m$ 是 w 在 $\mathbb{Q}$ 上的极小多项式, $f(x)$ 的全部根为 $w=w_1, w_2, \cdots, w_m$. 由于 $w^n=1$, 从而 $f(x)\mid x^n-1$, 于是 w 的每个共轭元

素也均满足 $w_i^n=1$，即 w_i 均是 n 次单位根. 于是 $|w_i|=1(1\leqslant i\leqslant m)$. 由韦达定理可知 $|c_i|\leqslant\binom{m}{i}(1\leqslant i\leqslant m)$. 另一方面，$f(x)$ 是 x^n-1 的首 1(即最高项系数为 1) 的多项式因子，由此不难证明 $f(x)\in\mathbb{Z}[x]$，即系数 c_i 均为有理整数. 进而，由于 $w\in K$，可知 $m=\deg f=[\mathbb{Q}(w):\mathbb{Q}]\leqslant[K:\mathbb{Q}]$. 但是次数 $\leqslant[K:\mathbb{Q}]$ 而有理整系数又有界 $|c_i|\leqslant\binom{m}{i}\leqslant\binom{[K:\mathbb{Q}]}{i}$ $(1\leqslant i\leqslant m)$ 的多项式 $f(x)$ 只有有限多个，从而它们的根也只有有限多个. 这就表明每个数域 K 中均只有有限多个单位根，即 W_K 是有限群. ▮

引理 5 任意域中的有限乘法群均是循环群.

证明 设 W 是域 K 中的有限乘法群. 令 $|W|=n$. 当 $n=1$ 时引理显然正确. 若 $n\geqslant 2$，令 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是不同的素数，$\alpha_i\geqslant 1$. 由于 W 是乘法 Abel 群. 根据有限 Abel 群的结构定理(附录 B, (1))，$W=W_1\times W_2\times\cdots\times W_s$(直积)，其中 W_i 是 W 的 $p_i^{\alpha_i}$ 阶 Sylow 子群 $(1\leqslant i\leqslant s)$. 于是 W_i 中每个元素 a 均满足 $a^{p_i^{\alpha_i}}=1$. 但是在域 K 中多项式 $x^{p_i^{\alpha_i-1}}-1$ 至多有 $p_i^{\alpha_i-1}$ 个根，从而在 W_i 中满足 $x^{p_i^{\alpha_i-1}}=1$ 的元素 x 也至多有 $p_i^{\alpha_i-1}$ 个. 这就表明 W_i 中存在 $p_i^{\alpha_i}$ 阶元素 $w_i(1\leqslant i\leqslant s)$. 由于 $p_1^{\alpha_1}, \cdots, p_s^{\alpha_s}$ 两两互素，因此 W 中元素 $w=w_1w_2\cdots w_s$ 的阶为 $p_1^{\alpha_1}\cdots p_s^{\alpha_s}=n=|W|$. 这就表明 W 是循环群. ▮

从以上两个引理立刻得出

定理 5 数域 K 中的单位根群 W_K 是有限循环群.

通常以 w_K 表示 K 中单位群 W_K 的阶.

例 1 如果 K 为实域，则 $W_K=\{\pm 1\}$, $w_K=2$.

例 2 设 $K=\mathbb{Q}(\sqrt{-d})$ 为虚二次域，d 为无平方因子的正整数. 则当 $d=1$ 时，$W_K=\{\pm 1, \pm\sqrt{-1}\}$, $w_K=4$; 当 $d=3$ 时，$W_K=\{\pm 1, \pm\omega, \pm\omega^2\}$, $\omega=e^{2\pi i/3}=\dfrac{1}{2}(-1+\sqrt{-3})$, $w_K=6$; 而当 $d>3$ 时，$W_K=\{\pm 1\}$, $w_K=2$. 这是因为：如果 $\zeta_n\in K$ 并且 n 有因子 p^m，则 $K\supseteq\mathbb{Q}(\zeta_n)\supseteq\mathbb{Q}(\zeta_{p^m})$，从而 $2=[K:\mathbb{Q}]\geqslant[\mathbb{Q}(\zeta_n):$

$\mathbb{Q}]\geqslant[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}]=p^{m-1}(p-1)$. 从而当 $p^{m-1}(p-1)\geqslant 3$ 时，K 中不可能包含 ζ_n，于是也就不能包含任何 n 次本原单位根. 所以能够在虚二次域 K 中的只能是 6 次和 3 次本原单位根(即上面的 $\pm\omega$ 和 $\pm\omega^2$，此时 $K=\mathbb{Q}(\sqrt{-3})$)，4 次本原单位根(即 $\pm\sqrt{-1}$，此时 $K=\mathbb{Q}(\sqrt{-1})$)和 ± 1.

对于每个正整数 n，$\zeta_n=e^{2\pi i/n}$ 是 n 次本原单位根，而 $\zeta_n^k(1\leqslant k\leqslant n,\ (k,n)=1)$ 就是全部 n 次本原单位根. 它们共有 $\varphi(n)$ 个，其中 $\varphi(n)$ 是欧拉函数，表示 $1,2,\cdots,n$ 当中与 n 互素的数的个数. $\varphi(n)$ 是积性函数，即当 $(n,m)=1$ 时，$\varphi(nm)=\varphi(n)\varphi(m)$. 由此及 $\varphi(p^a)=p^a-p^{a-1}=p^a\left(1-\dfrac{1}{p}\right)$ 就得到公式 $\varphi(n)=n\prod\limits_{p|n}\left(1-\dfrac{1}{p}\right)$.

现在我们考虑一般的分圆域 $\mathbb{Q}(\zeta_n)$，$\zeta_n=e^{2\pi i/n}$，n 是任意正整数. 为了计算这个域的次数，我们需要决定 ζ_n 的全部共轭元素.

引理 6 与 ζ_n 共轭的全部元素即是 $\varphi(n)$ 个 n 次本原单位根.

证明 ζ_n 的每个共轭元素均是某个域嵌入之下元素 ζ_n 的象，由此不难看出 ζ_n 的每个共轭元素均是 n 次本原单位根. 问题在于我们还需证明每个 n 次本原单位根均与 ζ_n 共轭. 为此我们只需证明：对于每个 n 次本原单位根 w 和素数 p，如果 $p\nmid n$，则 w^p 必然与 w 共轭. 因为如果这件事成立，就可以对于 k 归纳证明每个 n 次本原单位根 $\zeta_n^k(1\leqslant k\leqslant n,\ (n,k)=1)$ 均与 ζ_n 共轭.

设 $f(x)$ 为 w 在 $\mathbb{Q}$ 上的极小多项式. 由于 $w^n=1$，从而 $f(x)\mid x^n-1$. 令 $x^n-1=f(x)g(x)$. 因为 f 和 g 均是 x^n-1 的首 1 多项式因子，因此它们事实上均属于 $\mathbb{Z}[x]$ (习题 10). 现在假定 w^p 与 w 不共轭，则 $f(w^p)\neq 0$，于是 $g(w^p)=0$ (因为 $(w^p)^n-1=0$). 从而 w 是多项式 $g(x^p)$ 的根. 于是 $f(x)\mid g(x^p)$. 令 $g(x^p)=f(x)h(x)$. 由于 $g(x^p)$，$f(x)\in\mathbb{Z}[x]$，从而首 1 多项式 $h(x)$ 也属于 $\mathbb{Z}[x]$. 在环的自然同态 $\mathbb{Z}[x]\to((\mathbb{Z}/p\mathbb{Z}))[x]$ 之下，$\bar{f}(x)\mid\bar{g}(x^p)=\bar{g}(x)^p$. 由于 $(\mathbb{Z}/p\mathbb{Z})[x]$ 为唯一因子分解整区，从而上式表明 $(\bar{f}(x),\bar{g}(x))\neq 1$. 因此有多项式 $\bar{k}(x)\in(\mathbb{Z}/p\mathbb{Z})[x]$，$\deg\bar{k}(x)\geqslant 1$，使得 $\bar{k}(x)\mid(\bar{f}(x),\bar{g}(x))$. 于是 $\bar{k}^2(x)\mid\bar{f}\cdot\bar{g}=x^n-\bar{1}$. 但这是不可能的，因为当 $p\nmid n$ 时

$(\mathbb{Z}/p\mathbb{Z})[x]$ 中多项式 $x^n-\bar{1}$ 没有重根(附录 B, (10)). 这一矛盾表明 w^p 与 w 共轭. 从而也就证明了引理 6. ▌

定理 6 (1) $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$, 并且 $\zeta_n=e^{2\pi i/n}$ 在 $\mathbb{Q}$ 上的极小多项式为 $\Phi_n(x)=\sum\limits_{\substack{k=1\\(n,k)=1}}^{n}(x-\zeta_n^k)\in\mathbb{Z}[x]$.

(2) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 为伽罗华扩张, 并且其伽罗华群自然同构于 $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

证明 (1) $\Phi_n(x)\in\mathbb{Z}[x]$ 是由于它是 x^n-1 的首 1 多项式因子. 其余均由引理 6 推出.

(2) 由于 ζ_n 的全部共轭元素均属于 $K=\mathbb{Q}(\zeta_n)$, 从而 $K/\mathbb{Q}$ 是伽罗华扩张. 令 $\sigma_k\in \mathrm{Gal}(K/\mathbb{Q})$, 使得 $\sigma_k(\zeta_n)=\zeta_n^k$, $(n, k)=1$, 则 $\sigma_k\sigma_{k'}(\zeta_n)=\sigma_k(\zeta_n^{k'})=\zeta_n^{k'k}=\sigma_{kk'}(\zeta_n)$, 因此 $\sigma_k\sigma_{k'}=\sigma_{kk'}$. 所以映射

$$\chi:\ \mathrm{Gal}(K/\mathbb{Q})\to(\mathbb{Z}/n\mathbb{Z})^{\times},\ \chi(\sigma_k)=\bar{k}$$

是群的满同态. 但是由引理 6 $|\mathrm{Gal}(K/\mathbb{Q})|=[K:\mathbb{Q}]=\varphi(n)=|(\mathbb{Z}/n\mathbb{Z})^{\times}|$, 从而 χ 是同构. ▌

当 $n\equiv 2\ (\mathrm{mod}\ 4)$ 时, $\zeta_n=-\zeta_n^{(1+n)/2}=\zeta_{n/2}^{\frac{n+2}{4}}$. 因此 $\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{n/2})$. 所以通常对于分圆域 $\mathbb{Q}(\zeta_n)$, 可规定 $n\not\equiv 2\,(\mathrm{mod}\ 4)$. 在这一规定下, 不难证明当 $n\neq n'$ 时 $\mathbb{Q}(\zeta_n)\neq\mathbb{Q}(\zeta_{n'})$(习题 8), 并且也不难决定分圆域的单位根群(习题 9).

习　　题

1. 证明: 代数数集合是可数的, 而超越数集合是不可数的.

2. (a) 求证每个二次(数)域均可表达成 $\mathbb{Q}(\sqrt{d})$, 其中 d 是无平方因子整数;

(b) 如果 d 和 d' 均是无平方因子整数, 并且 $d\neq d'$, 则 $\mathbb{Q}(\sqrt{d})\neq\mathbb{Q}(\sqrt{d'})$;

(c) 二次域 K 必然是 $\mathbb{Q}$ 的伽罗华扩张. 试求其伽罗华群.

3. (a) 求下列代数数的次数和(在 $\mathbb{Q}$ 上的)极小多项式:

$\sqrt{2}+\sqrt{3}+\sqrt{5}$, $\sqrt{2+\sqrt{2}}$, $\sqrt[3]{2}+\omega$(其中 $\omega=e^{2\pi i/3}$);

(b) 求元素 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 的全部 $\mathbb{Q}(\sqrt{30})$ 中的共轭元素.

4. 证明代数数全体组成的集合 Ω 是域, 并且是有理数域 $\mathbb{Q}$ 的无限(次)代数扩域.

5. 对于数域 $L=\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$ 和 $L=\mathbb{Q}(\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{5})$, 求元素 γ, 使得 $L=\mathbb{Q}(\gamma)$.

6. 设 $f(x)\in K[x]$ 是数域 K 上的 n 次不可约首 1 多项式, $\alpha_1, \cdots, \alpha_n$ 是它的 n 个根, 称 $d(f)=\prod\limits_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2$ 是多项式 $f(x)$ 的判别式.

   (a) 求证 $d(f)$ 是 K 中元素;

   (b) 设 $f(x)=x^n+a$, $a\in\mathbb{Q}$, $\sqrt[n]{-a}\notin\mathbb{Q}$, 求证
   $$d(f)=(-1)^{n(n-1)/2}n^n a^{n-1};$$

   (c) 设 $f(x)=x^n+ax+b$ 是 $\mathbb{Q}[x]$ 中不可约多项式, 求证 $d(f)=(-1)^{n(n-1)/2}[(-1)^{n-1}(n-1)^{n-1}a^n+n^nb^{n-1}]$(注: 当 $n=2$ 和 3 时, $d(f)$ 分别为 a^2-4b 和 $-(4a^3+27b^2)$, 这就是 2 次和 3 次多项式通常所谓的判别式).

7. 求证: 一个代数整数是单位根的充要条件是它的每个共轭元素的绝对值均是 1.

8. 如果 $n\neq n'$, $n\not\equiv 2(\mathrm{mod}\ 4)$, $n'\not\equiv 2(\mathrm{mod}\ 4)$, 求证 $\mathbb{Q}(\zeta_n)\neq\mathbb{Q}(\zeta_{n'})$.

9. 令 $K=\mathbb{Q}(\zeta_n)$, 则

   (a) 当 $n\equiv 1(\mathrm{mod}\ 2)$ 时, $W_K=\{\zeta_{2n}^k\,|\,0\leqslant k\leqslant 2n-1\}$, $W_K=2n$;

   (b) 当 $n\equiv 0(\mathrm{mod}\ 4)$ 时, $W_K=\{\zeta_n^k\,|\,0\leqslant k\leqslant n-1\}$, $W_K=n$.

10. 如果 $f(x)$ 是 $\mathbb{Z}[x]$ 中的首 1 多项式, 而 $g(x)\in\mathbb{Q}[x]$ 是 $f(x)$ 的首 1 多项式因子, 求证 $g(x)\in\mathbb{Z}[x]$.

11. 设 $f(x)$ 为 $\mathbb{Q}[x]$ 中不可约首 1 多项式, $\alpha_1, \cdots, \alpha_n$ 是它的 n 个根, 令 $s_m=\sum\limits_{i=1}^{n}\alpha_i^m$, 求证
$$d(f)=\begin{vmatrix} s_0 & s_1\cdots s_{n-1} \\ s_1 & s_2\cdots s_n \\ \cdots\cdots \\ s_{n-1} & s_n\cdots s_{2n-2} \end{vmatrix}.$$

12. 设 $f(x)$ 是 $\mathbb{Q}[x]$ 中不可约首 1 多项式, 求证: 如果 $d(f)>0$, 则 $f(x)$ 有三个实根; 如果 $d(f)<0$, 则 $f(x)$ 只有 1 个实根.

13. 设 L/K 是数域的扩张. 对于 $\alpha\in L$, 定义映射
$$\varphi_\alpha:\ L\to L,\ \varphi_\alpha(\beta)=\alpha\beta.$$

   (a) 求证 φ_α 是 K-向量空间 L 中的线性变换;

   (b) 如果 A_α 是线性变换 φ_α 对于向量空间 L 的任意一组 K-基的变换

方阵，求证 $N_{L/K}(\alpha)=|A_\alpha|$，$T_{L/K}(\alpha)=T_r(A_\alpha)$（其中 $T_r(A)$ 表示方阵 A 的迹）.

§2 代数整数环

2.1 代数整数

在这一节中，我们要把有理数域 $\mathbb{Q}$ 中的整数概念推广到任意代数数域上去.

定义 1 代数数 α 叫作是**代数整数**(简称作**整数**)，如果存在一个系数属于 $\mathbb{Z}$ 的首1多项式 $f(x)$，使得 $f(\alpha)=0$.

例 1 每个 $n\in\mathbb{Z}$ 均是代数整数，因为它是首1多项式 $x-n\in\mathbb{Z}[x]$的根. 为了明确起见，今后我们将通常 $\mathbb{Z}$ 中的整数称作是**有理整数**，以区别于一般的代数整数.

例 2 n 次单位根是(代数)整数，因为它是首1多项式 $x^n-1\in\mathbb{Z}[x]$ 的根.

引理 7 设 α 为代数数，$f(x)$为 α 在 $\mathbb{Q}$ 上的极小多项式. 则 α 为整数的充要条件是 $f(x)\in\mathbb{Z}[x]$.

证明 由于极小多项式 $f(x)$是首1的. 所以若 $f(x)\in\mathbb{Z}[x]$，则由定义1和 $f(\alpha)=0$ 即知 α 是整数. 反之，如果 α 是整数，则存在首1多项式 $g(x)\in\mathbb{Z}[x]$，使得 $g(\alpha)=0$. 于是 $f(x)$是 $g(x)$的首1多项式因子，从而由§1，习题10即知 $f(x)\in\mathbb{Z}[x]$. ▮

系 $\mathbb{Q}$ 中只有有理整数才是(代数)整数.

证明 如果 $\alpha\in\mathbb{Q}$，$\alpha\notin\mathbb{Z}$，则 α 在 $\mathbb{Q}$ 上的极小多项式 $x-\alpha\notin\mathbb{Z}[x]$，由引理7知 α 不是(代数)整数. ▮

现在我们来决定二次域中的全部整数.

定理 7 以 O_K 表示二次域 $K=\mathbb{Q}(\sqrt{d})$(d 是无平方因子的有理整数)中的全部整数所组成的集合. 则当 $d\equiv2,3 \pmod 4$ 时，$O_K=\{a+b\sqrt{d}\,|\,a,\ b\in\mathbb{Z}\}$；而当 $d\equiv1 \pmod 4$时，$O_K=\{a+bw\,|\,a,\ b\in\mathbb{Z}\}$，其中 $w=\frac{1}{2}(1+\sqrt{d})$.

证明 K 中每个2次代数数 $\alpha+\beta\sqrt{d}$ ($\alpha,\ \beta\in\mathbb{Q},\ \beta\neq0$)的极

小多项式为 $x^2-2\alpha x+\alpha^2-\beta^2 d$. 因此(引理 7)

$\alpha+\beta\sqrt{d}$ 为整数 $\Leftrightarrow 2\alpha,\ \alpha^2-\beta^2 d\in\mathbb{Z}$.

而当 $\beta=0$ 时,易知这件事也是正确的.

设 $\alpha+\beta\sqrt{d}$ $(\alpha,\ \beta\in\mathbb{Q})$ 是整数, 则 $2\alpha,\ \alpha^2-\beta^2 d\in\mathbb{Z}$. 于是 $(2\alpha)^2-(2\beta)^2 d\in 4\mathbb{Z}$. 特别地, $(2\beta)^2 d\in\mathbb{Z}$. 由于 d 没有平方因子, 可知 $2\beta\in\mathbb{Z}$.

当 $d\equiv 2,\ 3 \pmod 4$ 时, 如果 2α 和 2β 均为奇数, 则 $(2\alpha)^2\equiv 1\not\equiv d\equiv(2\beta)^2 d \pmod 4$, 这与 $(2\alpha)^2-(2\beta)^2 d\in 4\mathbb{Z}$ 相矛盾. 因此 2α 和 2β 必有一为偶数. 然后由 $(2\alpha)^2\equiv(2\beta)^2 d \pmod 4$ 和 $d\not\equiv 0 \pmod 4$, 可知另一个亦为偶数. 即 $\alpha,\ \beta\in\mathbb{Z}$. 反之, 若 $\alpha,\ \beta\in\mathbb{Z}$, 显然 2α, $\alpha^2-\beta^2 d\in\mathbb{Z}$, 从而 $\alpha+\beta\sqrt{d}$ 为整数. 这就证明了定理的前半部分.

当 $d\equiv 1 \pmod 4$ 时, 由 $(2\alpha)^2\equiv(2\beta)^2 d\equiv(2\beta)^2 \pmod 4$ 可知有理整数 2α 和 2β 有相同的奇偶性. 于是 $\alpha-\beta\in\mathbb{Z}$, 而 $\alpha+\beta\sqrt{d}=(\alpha-\beta)+2\beta w$ (注意 $\sqrt{d}=2w-1$), 其中 $\alpha-\beta,\ 2\beta\in\mathbb{Z}$. 反之, 若 $a,\ b\in\mathbb{Z},\ b\neq 0$, 则 $a+bw=a+\frac{b}{2}+\frac{b}{2}\sqrt{d}$ 的极小多项式为 $x^2-(2a+b)+\left(a+\frac{b}{2}\right)^2-\frac{b^2}{4}d$, 其中 $2a+b\in\mathbb{Z}$, $\left(a+\frac{b}{2}\right)^2-\frac{b^2}{4}d=a^2+ab+b\cdot\frac{1-d}{4}\in\mathbb{Z}$. 从而 $a+bw\,(b\neq 0)$ 为整数. 而 $b=0$ 时这当然也对. 这就证明了定理的后半部分. ∎

2.2 代数整数环

对于二次域 K, 可以直接验证定理 7 中求出的整数集合 O_K 事实上是 K 的子环! 对于任意的数域 K, Dedekind 证明了 K 的整数集合 O_K 也是 K 的子环. 换句话说, 如果 α 和 β 均是 K 中的整数, 则 $\alpha\pm\beta$ 和 $\alpha\beta$ 亦是整数. 这是一件不平凡的事情($\sqrt{7}$, ζ_{89}, $\sqrt[3]{5}$, ζ_{61} 显然均是 $K=\mathbb{Q}(\sqrt{7},\ \sqrt[3]{5},\ \zeta_{89},\ \zeta_{61})$ 中的整数, 设想一下如何证明 $(\sqrt{7}+\zeta_{89})(\sqrt[3]{5}-\zeta_{61})$ 也是整数!). 我们需要给出整数的其他刻划方式.

定理 8 对于 $\alpha\in\mathbb{C}$，下面几个条件彼此等价：

(1) α 为(代数)整数；

(2) 环 $\mathbb{Z}[\alpha]$ 的加法群是有限生成的；

(3) α 是 $\mathbb{C}$ 的某个非零子环 R 中的元素，并且 R 的加法群是有限生成的；

(4) 存在有限生成非零加法子群 $A\subset\mathbb{C}$，使得 $\alpha A\subseteq A$.

证明 (1)⇒(2)：如果 α 为整数，由引理 7 知它的极小多项式 $f(x)$ 是系数属于 $\mathbb{Z}$ 的首 1 多项式，即 $f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$，$c_i\in\mathbb{Z}$. 于是 $\alpha^n=-c_{n-1}\alpha^{n-1}-\cdots-c_1\alpha-c_0$. 由此不难看出(对 m 归纳)，每个元素 α^m $(m\geqslant 0)$ 均可写成 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 的 $\mathbb{Z}$-线性组合，于是环 $\mathbb{Z}[\alpha]$ 中的每个元素也都如此. 这就表明环 $\mathbb{Z}[\alpha]$ 的加法群是由有限个元素 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 生成的.

(2)⇒(3)：取 $R=\mathbb{Z}[\alpha]$.

(3)⇒(4)：取 $A=R$.

(4)⇒(1)：设 $a_1, \cdots, a_n$ 生成加法群 A. 由于 $\alpha A\subseteq A$，每个 αa_i 均可表成 $a_1, \cdots, a_n$ 的 $\mathbb{Z}$-线性组合，我们可以把这写成矩阵形式

$$\begin{pmatrix}\alpha a_1\\ \vdots\\ \alpha a_n\end{pmatrix}=M\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix},$$

其中 M 是元素属于 $\mathbb{Z}$ 的 n 阶方阵. 此方程也可写成

$$(\alpha I_n-M)\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix},$$

由于 $A\neq(0)$，从而 $a_1, \cdots, a_n$ 不全为零. 由线性代数便知 $|\alpha I_n-M|=0$. 但是 $f(x)=|xI_n-M|$ 恰好是系数属于 $\mathbb{Z}$ 的 n 次首 1 多项式，并且 α 是它的根. 从而 α 是整数. ∎

定理 9 若 α 和 β 均是整数，则 $\alpha\pm\beta$, $\alpha\beta$ 也是整数. 特别地，数域 K 中全部整数组成的集合 O_K 是 K 的子环.

证明 根据定理 8，(2)，环 $\mathbb{Z}[\alpha]$ 和 $\mathbb{Z}[\beta]$ 的加法子群均是有

限生成的．设它们分别由$\{\alpha_1, \cdots, \alpha_n\}$和$\{\beta_1, \cdots, \beta_m\}$所生成的，则每个$\alpha^u (u\geqslant 0)$均可表为$\alpha_1, \cdots, \alpha_n$的$\mathbb{Z}$-线性组合，而每个$\beta^v (v\geqslant 0)$均可表为$\beta_1, \cdots, \beta_m$的$\mathbb{Z}$-线性组合．于是$\alpha^u\beta^v$均可表为$\{\alpha_i\beta_j\}_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m}$的$\mathbb{Z}$-线性组合，从而环$\mathbb{Z}[\alpha, \beta]$中每个元素均是如此，这就表明环$\mathbb{Z}[\alpha, \beta]$的加法群是有限生成的．但是$\alpha\pm\beta$, $\alpha\beta$均是$\mathbb{Z}[\alpha, \beta]$中元素，根据定理8，(3)可知它们均是整数． ▌

今后将O_K叫作是数域K的（代数）整数环．根据定理6的系，可知有理数域$\mathbb{Q}$的整数环就是$\mathbb{Z}$，而二次域的整数环已由定理7求出．现在我们来求分圆域$\mathbb{Q}(\zeta_{p^n})$的整数环（一般分圆域$\mathbb{Q}(\zeta_m)$的整数环见下一小节）．

定理10 分圆域$K=\mathbb{Q}(\zeta_{p^n})$的整数环是$\mathbb{Z}[\zeta_{p^n}]$．

证明 令$w=\zeta_{p^n}$, $s=\varphi(p^n)=[K:\mathbb{Q}]$．由于$w$为整数，从而由定理9可知$\mathbb{Z}[w]$中元素均为整数，即$\mathbb{Z}[w]\subseteq O_K$．为证$\mathbb{Z}[w]\supseteq O_K$，我们首先注意，由于$1, w, \cdots, w^{s-1}$是向量空间$K$的一组基，从而$K$中每个整数$\alpha$均可表成

$$\alpha=t_0+t_1w+\cdots+t_{s-1}w^{s-1}, \quad t_i\in\mathbb{Q}, \tag{1}$$

我们的目的是要证明$t_i\in\mathbb{Z} (0\leqslant i\leqslant s-1)$．

令$\mathrm{Gal}(K/\mathbb{Q})=\{\tau_1, \tau_2, \cdots, \tau_s\}$．将自同构$\tau_i$作用于(1)式上，得到

$$\tau_i(\alpha)=t_0+t_1\tau_i(w)+\cdots+t_{s-1}\tau_i(w^{s-1}) \quad (1\leqslant i\leqslant s).$$

由 Cramor 法则可得到$t_j=\gamma_j/\delta$，其中$\delta=\left|(\tau_i(w^k))_{\substack{1\leqslant i\leqslant s\\ 0\leqslant k\leqslant s-1}}\right|$，而$\gamma_j$是将$(\tau_1(\alpha), \cdots, \tau_s(\alpha))$代替方阵$(\tau_i(w^k))$的第$j$列而得到的新方阵的行列式．由于$\tau_i(w^k)$, $\tau_i(\alpha)$均是整数（习题1），从而γ_j和δ均是整数（定理9），并且事实上由上一小节的例题知道：

$$\delta^2=d_K(1, w, \cdots, w^{s-1})=(-1)^{\varphi(p^n)/2}p^{p^{n-1}(np-n-1)}.$$

令$\delta^2=d$，则$\delta\gamma_j=t_jd\in\mathbb{Q}$．但是$\delta\gamma_j\in O_K$，因此$\delta\gamma_j\in O_K\cap\mathbb{Q}=\mathbb{Z}$．于是$t_jd\in\mathbb{Z}$．令$t_jd=m_j\in\mathbb{Z}$，则(1)式可写成

$$\alpha=\frac{m_0}{d}+\frac{m_1}{d}w+\cdots+\frac{m_{s-1}}{d}w^{s-1}, \quad m_j\in\mathbb{Z}.$$

经过一个简单的变换，可以将上式改成

$$\alpha=\frac{m_0'}{d}+\frac{m_1'}{d}(1-w)+\cdots+\frac{m_{s-1}'}{d}(1-w)^{s-1},\quad m_j'\in\mathbb{Z}.\quad(2)$$

我们的目的是要证 $d|m_j(0\leqslant j\leqslant s-1)$，易知这等价于要证 $d|m_j'$ $(0\leqslant j\leqslant s-1)$. 现在假定 $m_j'(0\leqslant j\leqslant s-1)$ 不全被 d 除尽. 注意 $|d|=p^l$, $l=p^{n-1}(np-n-1)$, 从而若 $(m_0', m_1', \cdots, m_{s-1}')=p^\lambda\cdot m'$, $p\nmid m$, 则必然 $\lambda+1\leqslant l$. 于是令 $m_j'=\pm p^\lambda m_j''$, 则 $p\nmid(m_0'', m_1'', \cdots, m_{s-1}'')=m$. 从而存在整数 t, $0\leqslant t\leqslant s-1$, 使得 $p|m_j''(0\leqslant j\leqslant t-1)$, 但是 $p\nmid m_t''$. 于是(2)式可改写为

$$\pm p^{l-\lambda-1}\alpha-\left(\frac{m_0''}{p}+\frac{m_1''}{p}(1-w)+\cdots+\frac{m_{t-1}''}{p}(1-w)^{t-1}\right)$$
$$=\frac{m_t''}{p}(1-w)^t+\cdots+\frac{m_{s-1}''}{p}(1-w)^{s-1}.\qquad(3)$$

而(3)式左边仍为整数，记为 α'. 现在利用我们已经证得的公式 $N_{K/\mathbb{Q}}(1-w)=\prod\limits_{\substack{k=1\\p\nmid k}}^{p^n}(1-w^k)=p$. 由于 $(1-w^k)=(1-w)(1+w+\cdots+w^{k-1})$, 从而在环 $\mathbb{Z}[w]$ 中 $(1-w)|(1-w^k)(1\leqslant k\leqslant p^n-1)$. 于是 $(1-w)^s\left|\prod\limits_{\substack{k=1\\p\nmid k}}^{p^n}(1-w^k)=p\right.$. 因此 $p/(1-w)^s\in\mathbb{Z}[w]\subseteq O_K$. 由于 $t\leqslant s-1$, 从而由(3)式给出

$$\alpha'\cdot p/(1-w)^{t+1}=\frac{m_t''}{(1-w)}$$
$$+m_{t+1}''+\cdots+m_{s-1}''(1-w)^{s-1-t-1}\in O_K.$$

从而 $m_t'/(1-w)\in O_K$, 于是 $N_{K/\mathbb{Q}}(m_t''/(1-w))=m_t''^s/p\in O_K\cap\mathbb{Q}=\mathbb{Z}$. 但是这与 $p\nmid m_t''$ 相矛盾. 这一矛盾表明 $d|m_j'(0\leqslant j\leqslant s-1)$, 从而 $d|m_j(0\leqslant j\leqslant s-1)$, 即 $\alpha\in\mathbb{Z}[w]$. 于是 $O_K\subseteq\mathbb{Z}[w]$, 从而 $O_K=\mathbb{Z}[w]$. ▌

2.3 整基，数域的判别式

现在进一步研究整数环 O_K 的加法群结构. 我们要证明它是秩为 $[K:\mathbb{Q}]$ 的自由 Abel 群.

定义 2 群 G 叫作是秩为 n 的自由 Abel 群，如果它同构于 n

个有理整数加法群 $\mathbb{Z}$ 的直和: $G\cong\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$($n$ 个). 换句话说, 即存在 G 中 n 个元素 $\alpha_1, \cdots, \alpha_n$, 使得 G 中每个元素均可唯一地表示成 $m_1\alpha_1+\cdots+m_n\alpha_n$, $m_i\in\mathbb{Z}$. 这可以写成 $G=\mathbb{Z}\alpha_1\oplus\mathbb{Z}\alpha_2\oplus\cdots\oplus\mathbb{Z}\alpha_n$. 注意零群(0)看成是秩为 0 的自由 Abel 群.

定理 11 数域 K 的整数环 O_K 是秩 $n=[K:\mathbb{Q}]$ 的自由 Abel 群. 换句话说, 存在 $\omega_1, \cdots, \omega_n\in O_K$, 使得 $O_K=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$.

证明 设 $\alpha_1, \cdots, \alpha_n$ 是向量空间 K 的一组 $\mathbb{Q}$-基. 我们可以找到一个有理整数 $0\neq M\in\mathbb{Z}$, 使得 $M\alpha_i\in O_K(1\leqslant i\leqslant n)$ (习题 2), 于是 $M\alpha_i(1\leqslant i\leqslant n)$ 仍是 K 的一组 $\mathbb{Q}$-基, 所以我们一开始不妨就假定 $\alpha_i\in O_K(1\leqslant i\leqslant n)$, 从而每个整数 $\gamma\in O_K$ 均可写成

$$\gamma=x_1\alpha_1+\cdots+x_n\alpha_n,\quad x_i\in\mathbb{Q}.$$

令 $\sigma_1, \cdots, \sigma_n$ 是 K 到 $\mathbb{C}$ 中的 n 个嵌入, 则 $\sigma_i(\gamma)=x_1\sigma_i(\alpha_1)+\cdots+x_n\sigma_i(\alpha_n)\quad(1\leqslant i\leqslant n)$. 象定理 10 的证明那样, 由这些等式可以得出

$$x_j=\gamma_j/\delta,\ \delta=|(\sigma_i(\alpha_j))|,$$
$$\delta^2=d=d_K(\alpha_1, \cdots, \alpha_n)\in\mathbb{Z},\ \gamma_j\in O_K.$$

由于 $\alpha_1, \cdots, \alpha_n$ 是 $\mathbb{Q}$-线性无关的, 因此 $d\neq0$, 从而 $\delta\neq0$, 并且 δ 是整数. 于是 $\gamma_j\delta=x_jd\in\mathbb{Q}\cap O_K=\mathbb{Z}$. 令 $\gamma_j\delta=m_j$, 则 $x_j=m_j/d$ $(1\leqslant j\leqslant n)$. 这就表明 $\gamma\in\mathbb{Z}\frac{\alpha_1}{d}\oplus\cdots\oplus\mathbb{Z}\frac{\alpha_n}{d}$, 从而 $O_K\subseteq\mathbb{Z}\frac{\alpha_1}{d}\oplus\cdots\oplus\mathbb{Z}\frac{\alpha_n}{d}$. 但是右边是秩 n 的自由 Abel 群, 从而它的子群 O_K 是秩 $\leqslant n$ 的自由 Abel 群(附录 B, (1)). 最后, 由于 O_K 中存在着 $\mathbb{Z}$-线性无关的 n 个元素 $\alpha_1, \cdots, \alpha_n$, 因此加法群 O_K 的秩必然是 n, 这就完全证明了定理 11. ∎

定义 3 设 $\omega_1, \cdots, \omega_n\in O_K$, 如果 $O_K=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$, 则称 $\omega_1,\cdots,\omega_n$ 是整数环 O_K 或者数域 K 的一组整基, 换句话说, $\omega_1,\cdots,\omega_n$ 是 K 或 O_K 的一组整基, 当且仅当每个整数 $\alpha\in O_K$ 均可唯一地表示成 $\alpha=\lambda_1\omega_1+\cdots+\lambda_n\omega_n$, $\lambda_i\in\mathbb{Z}$.

定理 11 表明每个数域均存在整基, 但是并不是唯一的. 例如由定理 7 可知, 对于二次域 $K=\mathbb{Q}(\sqrt{d})$ ($d\in\mathbb{Z}$, 无平方因子), 当

$d\equiv 2,\ 3 \pmod 4$时，$\{1,\ \sqrt{d}\}$是域 K 的整基；而当 $d\equiv 1 \pmod 4$ 时，$\{1,\ w=(1+\sqrt{d})/2\}$是域 K 的整基. 另一方面，如果我们令

$$D=\begin{cases} d,\ d\equiv 1 \pmod 4\text{时}; \\ 4d,\ d\equiv 2,\ 3 \pmod 4\text{时}. \end{cases}$$

不难验证，在任何情形下，$\{1,\ (D+\sqrt{D})/2\}$也是域$\mathbb{Q}(\sqrt{d})$的整基. 又由定理 10 可知，分圆域 $\mathbb{Q}(\omega)(\omega=\zeta_{p^n})$ 的整数环是 $\mathbb{Z}[w]$，从而 $1,\ \omega,\ \cdots,\ \omega^{\varphi(p^n)-1}$是域 $\mathbb{Q}(\omega)$的整基，而 $1,(1-\omega),(1-\omega)^2,\ \cdots,\ (1-\omega)^{\varphi(p^n)-1}$也是域 $\mathbb{Q}(\omega)$的一组整基.

假设 $\beta_1,\cdots,\ \beta_n$ 和 $\gamma_1,\ \cdots,\gamma_n$ 均是数域 K 的整基. 从整基的定义可知存在元素属于 $\mathbb{Z}$ 的两个非异方阵 M 和 N，使得

$$\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}=M\begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_n\end{pmatrix},\quad \begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_n\end{pmatrix}=N\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix},$$

于是 $M=N^{-1}$，并且$|M|=|N|=\pm 1$. 若令 $\sigma_1,\ \cdots,\ \sigma_n$ 是 K 到 $\mathbb{C}$ 中的 n 个嵌入，$n=[K:\mathbb{Q}]$. 不难看出$(\sigma_i(\beta_j))=M(\sigma_i(\gamma_j))$. 从而

$$d_K(\beta_1,\ \cdots,\ \beta_n)=|M|^2\cdot d_K(\gamma_1,\ \cdots,\ \gamma_n)=d_K(\gamma_1,\ \cdots,\ \gamma_n).$$

这表明不同的整基有相同的判别式，即它是域 K（或环 O_K）本身的不变量，我们将它称作是域 K 的判别式，表示成 $d(K)$. 由于每组整基都是 $\mathbb{Z}$-线性无关的，从而也是 $\mathbb{Q}$-线性无关的，从而它们也是向量空间 K 的一组基. 于是它们的判别式不为零，即 $d(K)$ 是非零有理整数.

例 1 我们刚刚说过，$\{1,\ (D+\sqrt{D})/2\}$ 是二次域 $K=\mathbb{Q}(\sqrt{d})$的一组整基，其中 $D=\begin{cases} d,\ d\equiv 1 \pmod 4\text{时}; \\ 4d,\ d\equiv 2,\ 3 \pmod 4\text{时}. \end{cases}$ 于是

$$d(K)=\begin{vmatrix} 1 & \dfrac{D+\sqrt{D}}{2} \\ 1 & \dfrac{D-\sqrt{D}}{2} \end{vmatrix}^2=D.$$

例 2 由于$1,\omega,\omega^2,\cdots,\omega^{\varphi(p^n)-1}$是分圆域 $K=\mathbb{Q}(\omega)(\omega=\zeta_{p^n})$

的一组整基．从而令 $s=\varphi(p^n)=[K:\mathbb{Q}]$，则

$$d(K)=d_K(1,\ \omega,\ \cdots,\ \omega^{s-1})=(-1)^{s(s-1)/2}p^{p^{n-1}(np-n-1)}.$$

然而在一般情形下，寻求某个数域 K 的整基和计算判别式 $d(K)$ 并不是一件容易的事情．在这方面，下一个引理是有用的．

引理 8 设 $\alpha_1,\ \cdots,\ \alpha_n\in O_K$．如果

(1) $d_K(\alpha_1,\ \cdots,\ \alpha_n)=d(K)$；或者

(2) $d_K(\alpha_1,\ \cdots,\ \alpha_n)$ 是无平方因子的非零有理整数．

则 $\alpha_1,\ \cdots,\ \alpha_n$ 是域 K 的一组整基．

证明 设 $\omega_1,\ \cdots,\ \omega_n$ 是域 K 的一组整基，M 是用 $\omega_1,\ \cdots,\ \omega_n$ 表示整数 $\alpha_1,\ \cdots,\ \alpha_n$ 的有理整系数方阵，则

$$d_K(\alpha_1,\ \cdots,\ \alpha_n)=|M|^2\cdot d_K(\omega_1,\ \cdots,\ \omega_n)=|M|^2\cdot d(K).$$

如果 $d_K(\alpha_1,\ \cdots,\ \alpha_n)=d(K)$，则 $|M|=\pm1$．如果 $d_K(\alpha_1,\ \cdots,\ \alpha_n)$ 是无平方因子的非零有理整数，则也必然 $|M|=\pm1$．从而无论在哪种情形下，M 的逆方阵的系数仍属于 $\mathbb{Z}$，即 $\omega_1,\ \cdots,\ \omega_n$ 也可表示成 $\alpha_1,\ \cdots,\ \alpha_n$ 的 $\mathbb{Z}$-线性组合．这就表明 $\alpha_1,\ \cdots,\ \alpha_n$ 是域 K 的一组整基． ∎

例 x^5-x+1 是 $\mathbb{Q}[x]$ 中的不可约多项式（由于 $x^5-x+1\pmod 5$ 不可约，从而在 $\mathbb{Z}[x]$ 中不可约，于是在 $\mathbb{Q}[x]$ 中也不可约）．令 θ 是此多项式的一个根．则 $K=\mathbb{Q}(\theta)$ 为五次域．并且 $\theta\in O_K$．由 §1，习题 6 可算出

$$\begin{aligned}d_K(\theta)&=d_K(1,\ \theta,\ \theta^2,\ \theta^3,\ \theta^4)=N_{K/\mathbb{Q}}f'(\theta)\\&=4^4\cdot(-1)^5+5^5=19\cdot151.\end{aligned}$$

从而由引理 8，(2) 可知 $1,\ \theta,\ \theta^2,\ \theta^3,\ \theta^4$ 是域 $K=\mathbb{Q}(\theta)$ 的一组整基，并且 $O_K=\mathbb{Z}[\theta]$，$d(K)=19\cdot151$．

为了从一些域的整基得到它们的复合域的整基，有时可以利用下面的引理．

引理 9 设 K 和 L 均是数域，$[K:\mathbb{Q}]=m$，$[L:\mathbb{Q}]=n$，$[KL:\mathbb{Q}]=mn$，并且 $(d(K),\ d(L))=1$．则

(1) $O_{KL}=O_KO_L$；

(2) 若 $\{\alpha_1,\ \cdots,\ \alpha_m\}$ 和 $\{\beta_1,\ \cdots,\ \beta_n\}$ 分别是 K 和 L 的整基，则

$\{\alpha_i\beta_j \mid 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\}$是域 KL 的一组整基;

(3) $d(KL)=d(K)^n d(L)^m$.

证明 (1)和(2): 设$\{\alpha_1, \cdots, \alpha_m\}$和$\{\beta_1, \cdots, \beta_n\}$分别是 K 和 L 的整基, 可知 $KL=\mathbb{Q}(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n)$, 并且 KL 中每个元素均可表成$\{\alpha_i\beta_j \mid 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\}$的 $\mathbb{Q}$-线性组合. 特别地, 每个元素 $\alpha\in O_{KL}$ 均可表示成

$$\alpha=\sum_{i,j}\frac{r_{ij}}{r}\alpha_i\beta_j,\ r_{ij},\ r\in\mathbb{Z},\ (r,\ r_{11},\ \cdots,\ r_{mn})=1. \qquad (*)$$

我们现在要证明 $r\mid d(K)$. 为此, 考虑任意一个嵌入 σ_k: $K\to\mathbb{C}$. 它可以用$[KL:K]=[KL:\mathbb{Q}]/[K:\mathbb{Q}]=mn/m=n$ 种方式扩充成KL到 $\mathbb{C}$ 中的嵌入, 这 n 个扩充在 L 上的限制是彼此不同的(否则它们在 KL 上就是同样的嵌入了), 从而其中恰好有一个扩充是L-嵌入(即它在 L 上的限制为 L 上的恒等自同构). 我们将这个扩充仍记为 σ_k, 于是

$$\sigma_k(\alpha)=\sum_{i,j}\frac{r_{ij}}{r}\ \sigma_k(\alpha_i)\beta_j=\sum_{i=1}^{m}\sigma_k(\alpha_i)x_i,$$

$$x_i=\sum_{j=1}^{n}\frac{r_{ij}}{r}\ \beta_j \quad (1\leqslant i\leqslant m).$$

将 Cramor 法则用于上面m个方程$(1\leqslant k\leqslant m)$, 便解出

$$x_i=\gamma_i/\delta,\ \delta=|\sigma_k(\alpha_i)|,$$

其中 δ 和 γ_i 均为整数, $\delta^2=d(K)$. 于是 $d(K)x_i=\delta\gamma_i$ 为整数. 但是 $d(K)x_i=\sum_{j=1}^{n}\dfrac{d(K)r_{ij}}{r}\beta_j\in L$, 因此也属于 O_L. 由于$\{\beta_1, \cdots, \beta_n\}$为 L 的整基, 所以 $d(K)r_{ij}/r\in\mathbb{Z}$. 由 $(r_1, r_{11}, r_{12}, \cdots, r_{mn})=1$. 可知 $d(K)/r\in\mathbb{Z}$, 这就证明了 $r\mid d(K)$. 完全类似地可证 $r\mid d(L)\cdots$从而 $r\mid(d(K),\ d(L))=1$, 即 $r=\pm1$. 于是由$(*)$式即知每个元素 $\alpha\in O_{KL}$均可表成$\{\alpha_i\beta_j\}$的 $\mathbb{Z}$-线性组合. 由于$[KL:\mathbb{Q}]=mn=|\{\alpha_i\beta_j\}|$, 从而$\{\alpha_i\beta_j \mid 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\}$是 O_{KL} 的一组整基, 并且由此即得到$O_{KL}=O_KO_L$.

(3): 设 $\sigma_1, \cdots, \sigma_m$ 是 K 到 $\mathbb{C}$ 中的全部嵌入, $\tau_1, \cdots, \tau_n$ 是 L 到 $\mathbb{C}$ 中的全部嵌入. 我们在前面事实上证明了, 对于每一对$(\sigma_i,$

τ_j)，均存在唯一的嵌入 $\pi_{ij}: KL\to\mathbb{C}$，使得 $\pi_{ij}|_K=\sigma_i$，$\pi_{ij}|_L=\tau_j$，于是$\{\pi_{ij}|1\leqslant i\leqslant m, 1\leqslant j\leqslant n\}$就是 KL 到 $\mathbb{C}$ 的全部嵌入，因此

$$\begin{aligned}d(KL)&=|(\pi_{ij}(\alpha_\lambda\beta_\mu))|^2=|(\sigma_i(\alpha_\lambda)\tau_j(\beta_\mu))|^2\\&=|(\sigma_i(\alpha_\lambda))*(\tau_j(\beta_\mu))|^2,\end{aligned}$$

其中 $*$ 表示矩阵 $(\sigma_i(\alpha_\lambda))$ 和 $(\tau_j(\beta_\mu))$ 的 Kronecker 积. 由于 $|(\sigma_i(\alpha_\lambda))|^2=d(K)$，$|(\tau_j(\beta_\mu))|^2=d(L)$，由 Kronecker 积的行列式公式即知 $d(KL)=d(K)^n d(L)^m$. ▮

作为引理 9 的应用，我们来决定一般分圆域 $\mathbb{Q}(\zeta_m)$ 的整数环、整基和判别式.

定理 12 设 $K=\mathbb{Q}(\zeta_m)$，$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}\not\equiv 2\pmod 4$，其中 $p_1, \cdots, p_r$ 是不同的素数，$\alpha_i\geqslant 1$，则

(1) $O_K=\mathbb{Z}[\zeta_m]$，从而$\{1, \zeta_m, \cdots, \zeta_m^{\varphi(m)-1}\}$是域 K 的一组整基；

(2) $d(K)=(-1)^{\varphi(m)/2}m^{\varphi(m)}/\prod\limits_{p|m}p^{\varphi(m)/(p-1)}$.

证明 我们只证 $r=2$ 的情形，因为一般情形不难由此归纳出来. 设 $m=p_1^{\alpha_1}p_2^{\alpha_2}$、$K_1=\mathbb{Q}(\zeta_{p_1^{\alpha_1}})$、$K_2=\mathbb{Q}(\zeta_{p_2^{\alpha_2}})$，则 $K_1K_2=\mathbb{Q}(\zeta_{p_1^{\alpha_1}}, \zeta_{p_2^{\alpha_2}})=\mathbb{Q}(\zeta_{p_1^{\alpha_1}p_2^{\alpha_2}})=K$，$d(K_i)=(-1)^{\varphi(p_i^{\alpha_i})/2}(p_i^{\alpha_i})^{\varphi(p_i^{\alpha_i})}/p_i^{\varphi(p_i^{\alpha_i})/(p_i-1)}$ $(i=1, 2)$，从而$(d(K_1), d(K_2))=1$. 又有$[K:\mathbb{Q}]=\varphi(p_1^{\alpha_1}p_2^{\alpha_2})=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})=[K_1:\mathbb{Q}]\cdot[K_2:\mathbb{Q}]$. 因此引理 9 的条件全部满足. 从而 $O_K=\mathbb{Z}[\zeta_{p_1^{\alpha_1}}]\cdot\mathbb{Z}[\zeta_{p_2^{\alpha_2}}]=\mathbb{Z}[\zeta_{p_1^{\alpha_1}}, \zeta_{p_2^{\alpha_2}}]=\mathbb{Z}[\zeta_m]$，$d(K)=d(K_1)^{\varphi(p_2^{\alpha_2})}d(K_2)^{\varphi(p_1^{\alpha_1})}=(-1)^{\varphi(m)/2}m^{\varphi(m)}/\prod\limits_{p|m}p^{\varphi(m)/(p-1)}$. ▮

以上我们对于二次域和分圆域给出了它们的整基. 我们在下一章还要对纯三次域明显地给出整基. 对于任意数域 K，如何有效地给出整数环 O_K 的整基，是人们长期以来所关心的问题. 此外，人们对于以下一些特殊类型的整基感兴趣.

(1) 幂元整基　如果存在 $\alpha\in O_K$，使得$\{1, \alpha, \cdots, \alpha^{n-1}\}$是 n 次数域 K 的整基，即 $O_K=\mathbb{Z}\oplus\mathbb{Z}\alpha\oplus\cdots\oplus\mathbb{Z}\alpha^{n-1}$，便称域 K 具有幂元整基. 我们在下一章将看到这种幂元整基对于研究 O_K 中素理想分解所带来的好处. 从定理 7 和定理 12 可以看出，二次域和分

圆域均有幂元整基. 而 Dedekind 给出了不具有幂元整基的三次域的例子(习题 3). 哪些数域具有幂元整基?这一问题甚至对于循环三次数域均不清楚(注:数域 K 叫作是循环域,是指 $K/\mathbb{Q}$ 为伽罗华扩张,并且其伽罗华群是循环群).

(2) 正规整基 设 $K/\mathbb{Q}$ 是 n 次伽罗华扩张, $\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_1, \cdots, \sigma_n\}$,如果存在 $\alpha\in O_K$ 使得 $\{\sigma_1(\alpha), \cdots, \sigma_n(\alpha)\}$ 是 K 的整基,则称 K 具有**正规整基**. 一个伽罗华数域何时具有正规整基,这个问题也有一定的理论价值. 不难证明:二次域 K 有正规整基的充要条件是 $d(K)$ 为奇数(习题 10). 而分圆域 $\mathbb{Q}(\zeta_n)$ 有正规整基的充要条件是 n 为一些不同的素数之乘积. 对于其他类型的数域,能否给出存在正规整基的一个简单的充分必要条件?

(3) 相对整基 设 L/K 是数域的 n 次扩张. 如果存在 $\alpha_1, \cdots, \alpha_n\in O_L$, 使得 $O_L=\alpha_1 O_K\oplus\cdots\oplus\alpha_n O_K$, 则称 $\{\alpha_1, \cdots, \alpha_n\}$ 为扩张 L/K 的**相对整基**. 当 $K=\mathbb{Q}$ 时,这就是通常的整基,我们已经证明了这种情形下(相对)整基是存在的. 更一般地,可以证明,如果 O_K 是主理想环,则 L/K 的相对整基必然存在. 但是有许多例子表明,如果 O_K 不是主理想环,则 L/K 可以不具有相对整基. 对于 $L=\mathbb{Q}(\sqrt{d}, \sqrt{e})$, $K=\mathbb{Q}(\sqrt{d})$, $[L:K]=2$ 的情形,关于 L/K 的相对整基问题已有很完整的结果. 张贤科对于 L 为循环四次域而 K 为 L 的(唯一)二次子域的情形也给出了完整的答案. 对于其他情形则还没有完整的结果.

我们再谈谈关于判别式的一些问题:

(1) 哪些有理整数 d 可以是某个数域 K 的判别式 $d(K)$?一个必要条件是 $d\equiv 1$ 或 $0 \pmod 4$ (习题 5),但这不是充分条件. 例如 $-12, 4, 9$ 均不是数域的判别式.

(2) 以 $M(r_1, r_2)$ 表示全部具有 r_1 个实嵌入和 r_2 对虚嵌入的 n 次数域 K 当中 $(n=r_1+2r_2)$ 其判别式绝对值 $|d(K)|$ 的最小值. 对于二次域不难看出 $M(2, 0)=5$, $M(0, 1)=3$. 对于三次域, Davenport(1939 年)证明了 $M(3, 0)=49$ $(K=\mathbb{Q}(\theta), \theta^3+\theta^2-2\theta-1=0)$. 对于四次域, J. Mayer(1929 年)证明了 $M(0, 2)$

$=117$, $M(2, 1)=275$, $M(4, 0)=725$. 对于五次域, H. Cohn (1955年)证明了 $M(1, 2)=1609$, $M(3, 1)=4511$, $M(5, 0)=14641$.

(3) 令 $D_0=\lim\limits_{n\to\infty} M(n, 0)^{1/n}$, 目前关于 D_0 的下界的最好结果是 Poitou(1977年)的 $D_0\geqslant 60.83$. 进而我们定义

$D=\lim\limits_{n\to\infty} \mathrm{Min}\{M(r_1, r_2)^{1/n} | r_1+2r_2=n\}$. Mulholland(1960年)证明了 $D\geqslant 15.775$. 很长时期人们猜想 $D=+\infty$. 但是于1964年俄国数学家 Голод 和 Шафаревич 否定了关于类域塔的一个猜想的同时, 也否定了猜想 $D=+\infty$. 不久 A. Brumer (1965年)证明了 $D\leqslant 347$.

对于判别式的上下界的估计, 在研究代数数论许多问题(例如类数估计等)的时候都是有用的.

习 题

1. (a)如果 α 是(代数)整数, 求证 α 的每个共轭元素也是(代数)整数;
   (b) 设 L/K 是数域的扩张, 求证: $N_{L/K}(O_L)\subseteq O_K$, $T_{L/K}(O_L)\subseteq O_K$;
   (c) 设 L/K 是数域的扩张, $\alpha\in L$, 求证: $\alpha\in O_L \Leftrightarrow \alpha$ 在 K 上的极小多项式属于 $O_K[x]$.
2. 求证: 对于每个代数数 α, 均存在一个有理整数 $n\in\mathbb{Z}$, 使得 $n\alpha$ 是代数整数.
3. (Dedekind)(a) 证明 x^3+x^2-2x+8 是 $\mathbb{Q}[x]$中的不可约多项式. 令 θ 为此多项式的一个根, $K=\mathbb{Q}(\theta)$;
   (b) 证明 $d_K(1, \theta, \theta^2)=4\cdot 503$;
   (c) 证明 $\theta'=4/\theta\in O_K$, $\{1, \theta, \theta'\}$ 是域 K 的一组整基, 并且 $d(K)=503$;
   (d) 求证: 对于每个 $\alpha\in O_K$, $\{1, \alpha, \alpha^2\}$ 均不可能是域 K 的一组整基. (提示: 对每个 $\alpha\in O_K$, 证明 $d_K(1, \alpha, \alpha^2)$必为偶数.)
4. 对于每个数域 K, 求证 $(-1)^{r_2}d(K)>0$, 其中 r_2 表示域 K 的复嵌入有多少对.
5. (Stickelberger)对于每个数域 K, 求证 $d(K)\equiv 0$ 或者 $1 \pmod 4$.
6. 设 θ 是 $f(x)=x^3+5x+4$ 的一个根, $K=\mathbb{Q}(\theta)$, 求证 $d(K)=-4\cdot 233$,

7. 设 p 为奇素数, $\omega=\zeta_p$, $K=\mathbb{Q}(\omega)$,

(a) 求证 $K_0=\mathbb{Q}(\omega+\omega^{-1})$ 是 K 的极大实子域(即 K 的每个实子域均是 K_0 的子域), 并且 $[K_0:\mathbb{Q}]=(p-1)/2$;

(b) 求证 $O_{K_0}=\mathbb{Z}[\omega+\omega^{-1}]$, 并且 $\{\omega+\omega^{-1}, \omega^2+\omega^{-2}, \cdots, \omega^{\frac{p-1}{2}}+\omega^{-\frac{p-1}{2}}\}$ 是域 K_0 的一组整基;

(c) 计算域 $K_0=\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ 的判别式.

8. 写出前 11 个分圆多项式 $\Phi_m(x)(2\leqslant m\leqslant 12)$.

9. 利用代数整数的性质证明 § 1 中的习题 10.

10. 求证二次域 K 有正规整基的充要条件是 $d(K)$ 为奇数.

11. 如果 n 是一些不同的素数之乘积, 求证分圆域 $\mathbb{Q}(\zeta_n)$ 有正规整基.

第二章　整数环中的素理想分解

我们在前一章中介绍了整数环 O_K 的加法群结构. 这一章要研究环 O_K 的理想. 关于这个问题的历史,我们已经在前言中作了介绍. 那就是:库默尔在研究费尔马问题的时候发现(用今天的术语来说)环 O_K 可能不是唯一因子分解整环. 但是由库默尔发明而由 Dedekind 发展了的理想理论,证明了对于每个数域 K, 环 O_K 中每个理想均可唯一地写成有限个素理想的乘积. 后人把具有这样性质的(带 1 交换)整环称作是 Dedekind 整环. 本章首先证明 O_K 是 Dedekind 整环, 然后要花很大的篇幅对于 O_K 中理想的素理想分解特性作深入细致的探讨,作为应用,我们在 § 6 中证明了 Kronecker-Weber 定理.

§ 1　分解的存在唯一性

1.1　Dedekind 整环

定义 1　整环 R 叫作诺特(Noether)整环, 如果 R 的每个理想均是有限生成的.

注记　(1) 这里的"有限生成"是指理想而言, 不是象前一章指加法群而言. 具体说来,由环 R 中元素 $a_1, a_2, \cdots, a_n$ 生成的加法群为 $\mathbb{Z}a_1+\mathbb{Z}a_2+\cdots+\mathbb{Z}a_n$, 而生成的理想为 $Ra_1+Ra_2+\cdots+Ra_n$.

(2) 整环(domain)是无零因子的环(见附录), 而整数环的"整"(integral)如第一章所定义,不要因中文名称相近而混淆.

例如,主理想整环的每个理想均是由一元生成的(主理想),从而是诺特整环. 而无限个未定元的整环 $R=\mathbb{Z}[x_1, x_2, \cdots, x_n, \cdots]$ 不是诺特整环, 因为理想 $Rx_1+Rx_2+\cdots+Rx_n+\cdots$ 不是有限生成

的.

引理1 设 R 为整环,则以下三个条件彼此等价

(a) R 是诺特整环;

(b) (理想升链条件) 如果 $I_i(i=1, 2, \cdots)$ 均是 R 中理想,并且 $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$,则存在 $n_0\in\mathbb{Z}$,使得 $I_{n_0}=I_{n_0+1}=\cdots$;

(c) 设 S 是 R 中一些理想组成的非空集合,则 S 中存在极大元 I(即不存在 $I'\in S$,使得 $I'\supsetneqq I$).

证明

$(a)\Rightarrow(b)$: 令 $I=\bigcup_{i=1}^{\infty}I_i$,易知这也是 R 的理想,由(a)知它应当是有限生成的.设 I 是由元素 $x_1, \cdots, x_n$ 生成的,由于 $x_j\in I$, 从而 x_j 属于某个 $I_{i_j}(1\leqslant j\leqslant n)$, 令 $n_0=\max(i_1, \cdots, i_n)$, 则 $x_j\in I_{i_j}\subseteq I_{n_0}$ $(1\leqslant j\leqslant n)$. 于是 $I\subseteq I_{n_0}\subseteq I_{n_0+1}\subseteq\cdots\subseteq I$, 从而$I_{n_0}=I_{n_0+1}=\cdots$.

$(b)\Rightarrow(c)$: 用反证法即可.

$(c)\Rightarrow(a)$: 也用反证法. 假如 R 中理想 I 不是有限生成的.取 $x_1\in I$,则 $I_1=Rx_1$ 为 R 的理想,由于 I 不是有限生成的,从而 $I_1\subsetneqq I$. 于是有 $x_2\in I-I_1$. 又有理想 $I_2=Rx_1+Rx_2\subsetneqq I$. 如此下去便得到一个理想集合 $S=\{I_1, I_2, \cdots\}$, $I_n\subsetneqq I_{n+1}$,从而 S 中没有极大元,与(c)相矛盾. ▋

定义2 整环 R 叫作是整闭的, 是指若 a 属于 R 的商域 F,并且它是 $R[x]$ 中某个首1多项式的根,则必然 $a\in R$.

定义3 整环 R 叫作是 Dedekind 整环, 如果它满足如下三个条件

(1) R 是诺特整环;

(2) R 中每个非零素理想均是极大理想;

(3) R 是整闭的.

现在我们叙述 Dedekind 整环的一些简单性质, 其中最重要的是素理想分解定理. 以下所谓理想均指非零理想.

引理2 在诺特整环 R 中,对于每个理想 I,均存在 R 的有限个素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$,使得 $I\supseteq\mathfrak{p}_1\cdots\mathfrak{p}_n$.

证明 我们以 S 表示不具有引理所述性质的那些理想 I 所构成的集合. 如果 $S\neq\varnothing$(空集), 则由于 R 是诺特整环, S 中有极大元 M(引理 1). M 显然不是素理想(因为 M 不具有引理所述性质). 因此存在 $r, s\in R-M$, 使得 $rs\in M$. 于是理想 $M+Rr$ 和 $M+Rs$ 均真包含 M, 从而均不属于 S. 于是存在素理想 $\mathfrak{p}_1$, $\cdots$, $\mathfrak{p}_n$, $\mathfrak{q}_1$, $\cdots$, $\mathfrak{q}_m$, 使得 $M+Rr\supseteq\mathfrak{p}_1\cdots\mathfrak{p}_n$, $M+Rs\supseteq\mathfrak{q}_1\cdots\mathfrak{q}_m$. 从而 $M\supseteq(M+Rr)(M+Rs)\supseteq\mathfrak{p}_1\cdots\mathfrak{p}_n\mathfrak{q}_1\cdots\mathfrak{q}_m$. 这就与 $M\in S$ 相矛盾. 从而 $S=\varnothing$, 即 R 中每个理想均具有引理中所述性质. ▮

引理 3 设 A 是 Dedekind 整环 R 的理想, $A\neq R$. K 为 R 的商域, 则存在元素 $\gamma\in K-R$, 使得 $\gamma A\subseteq R$.

证明 对于 $0\neq a\in A$, 令 r 是最小正整数使得 $(a)\supseteq\mathfrak{p}_1\cdots\mathfrak{p}_r$, 其中 $\mathfrak{p}_i$ 均为 R 中的素理想(r 的存在性由引理 2 给出). 由于 A 必然包含在某个极大理想 $\mathfrak{m}$ 中, 从而 $\mathfrak{m}\supseteq A\supseteq\mathfrak{p}_1\cdots\mathfrak{p}_r$. 由于极大理想 $\mathfrak{m}$ 也是素理想, 因此 $\mathfrak{m}$ 必包含 $\mathfrak{p}_1$, $\cdots$, $\mathfrak{p}_r$ 中的某一个(为什么?), 不妨设 $\mathfrak{m}\supseteq\mathfrak{p}_1$, 但是在 Dedekind 整环中, 素理想也是极大理想, 于是 $\mathfrak{m}=\mathfrak{p}_1$. 另一方面, 由 r 的极小性可知有 $b\in\mathfrak{p}_2\cdots\mathfrak{p}_r$, $b\notin(a)$. 令 $\gamma=b/a$, 则 $\gamma\in K-R$, 并且 $bA\subseteq b\mathfrak{m}=b\mathfrak{p}_1\subseteq\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\subseteq aR$, 从而 $\gamma A\subseteq R$. ▮

引理 4 设 I 是 Dedekind 整环 R 中的理想, 则存在 R 中另一个理想 J, 使得 IJ 为主理想.

证明 取 $0\neq\alpha\in I$. 令 $J=\{\beta\in R\,|\,\beta I\subseteq(\alpha)\}$. J 显然是 R 的理想, 并且 $IJ\subseteq(\alpha)$. 从而 $A=\frac{1}{\alpha}IJ\subseteq R$ 并且 A 是 R 中理想. 如果 $A\neq R$ 我们来推出矛盾: 由引理 3 知存在 $\gamma\in K-R$, 使得 $\gamma A\subseteq R$. 由于 $\alpha\in I$, 从而 $A=\frac{1}{\alpha}IJ\supseteq J$, 于是 $\gamma J\subseteq\gamma A\subseteq R$. 对于每个 $\beta\in J$, 则 $\gamma\beta\in R$, 并且 $\gamma\beta I\subseteq\gamma JI=\gamma\alpha A\subseteq\alpha R=(\alpha)$. 从而由 J 的定义可知 $\gamma\beta\in J$, 于是 $\gamma J\subseteq J$. 由于 R 为诺特整环, 从而理想 J 是由有限个元素 α_1, $\cdots$, α_m 生成的. 由 $\gamma J\subseteq J$ 给出方程组

$$\gamma\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}=M\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix},$$

其中 M 是 R 上的 m 阶方阵. 由于 $\alpha_1, \cdots, \alpha_m$ 不全为零(因为 $J\neq(0)$), 从而由线性代数可知 $|\gamma I_m-M|=0$, 即 γ 是 $R[x]$ 中首 1 多项式 $|xI_m-M|$ 的根. 利用 R 的整闭特性, 可知 $\gamma\in R$. 这就与原来的 $\gamma\in K-R$ 相矛盾. 因此必然 $A=R$, 即 $IJ=(\alpha)$. ▌

引理 5 (消去律) 设 A, B, C 均为某个 Dedekind 整环中的理想, 则 $AB=AC\Rightarrow B=C$.

证明 由引理 4 可知存在理想 J, 使得 $AJ=(\alpha)$, $\alpha\neq0$, 于是 $\alpha B=ABJ=ACJ=\alpha C$. 由于 R 为整环, 即得 $B=C$. ▌

引理 6 设 A 和 B 为 Dedekind 整环 R 中两个理想, 则 $A\supseteq B\Leftrightarrow$ 存在 R 中理想 C, 使得 $B=AC$.

证明 $\Leftarrow$: 显然. $\Rightarrow$: 取理想 J, 使得 $AJ=(\alpha)$. 由 $A\supseteq B$ 可知 $C=\frac{1}{\alpha}JB$ 是 R 中理想, 并且 $B=AC$. ▌

现在我们可以证明 Dedekind 整环的重要性质.

定理 1 Dedekind 整环 R 中每个(非零)理想均可(不计次序)唯一地表成有限个素理想的乘积(规定 R 是 0 个素理想之积).

证明 (存在性) 令 S 为 R 中不能表成有限个素理想之积的那些理想组成的集合. 由定理中的规定知 $R\notin S$. 如果 $S\neq\varnothing$, 则 S 中有极大元 $M\neq R$, 从而 M 包含在某个极大理想(从而也是素理想) P 之中. 由引理 6 知有理想 I 使得 $M=PI$. 由引理 5 可知 $I\supsetneqq M$. 从而由 M 在集合 S 中的极大性可知 $I\notin S$. 于是 $I=P_1\cdots P_r$, 从而 $M=PP_1\cdots P_r$, 其中 P, P_i 均为 R 的素理想. 这就与 $M\in S$ 相矛盾. 因此必然 $S=\varnothing$, 即 R 中每个非零理想均可表成有限个素理想的乘积.

(唯一性) 假设 $P_1\cdots P_r=Q_1\cdots Q_s$, 其中 P_i, Q_j 均为 R 的素理想, 则 $P_1\supseteq Q_1\cdots Q_s$. 从而 P_1 包含 $Q_1, \cdots, Q_s$ 中的某一个. 不妨

设 $P_1\supseteq Q_1$，由于素理想 P_1 和 Q_1 均为极大理想，从而 $P_1=Q_1$. 然后由引理5中的消去律给出 $P_2\cdots P_r=Q_2\cdots Q_s$. 继续下去即知 $r=s$, 并且(必要时改动一下诸 Q_i 的下标) $P_i=Q_i(1\leqslant i\leqslant r)$. ∎

注记 可以证明定理1的逆也是成立的. 换句话说，我们也可把素理想分解式的存在唯一性作为 Dedekind 整环的定义.

基于定理1，我们可以把唯一因子分解整环中关于元素的许多性质推广到 Dedekind 整环 R 的理想上. 例如，我们可以定义 R 中理想 A 整除理想 B(表示成 $A|B$)，即指存在 R 的理想 C，使得 $B=AC$，这时 A 叫作 B 的(理想)因子，而 B 可以叫作是 A 的倍理想. 由引理6可知 $A|B$ 和 $A\supseteq B$ 是一回事(注意：若 A 为 B 的理想因子，则作为集合 A 比 B 要大！). 类似地可定义几个理想的最大公因子和最小公倍理想. 如果将理想 A 和 B 分解成素理想的乘积：

$$A=P_1^{e_1}\cdots P_r^{e_r},\ B=P_1^{f_1}\cdots P_r^{f_r},\ e_i,\ f_i\geqslant 0$$

(这里我们允许 e_i 或 f_i 为0，并且 $P_i^0=R$，是为了将 A 和 B 的分解式右边形式上有相同的一些素理想)，其中 $P_1,\cdots,P_r$ 是彼此不同的素理想. 容易看出：$A|B\Leftrightarrow e_i\leqslant f_i(1\leqslant i\leqslant r)$(习题2). 此外，若令 $t_i=\min(e_i,\ f_i)$，$m_i=\max(e_i,\ f_i)$，则 $P_1^{t_1}\cdots P_r^{t_r}$ 和 $P_1^{m_1}\cdots P_r^{m_r}$ 显然是 A 和 B 的最大公因子和最小公倍理想. 但是我们无须赋以新的符号，因为它们分别是 $A+B$ 和 $A\cap B$(习题2).

具有素理想唯一分解性质的整环何时才能具有元素的唯一分解性质，即一个 Dedekind 整环何时是唯一因子分解整环？下面引理给出答案.

引理7 设 R 为 Dedekind 整环，则 R 是唯一因子分解整环的充要条件为 R 是主理想整环.

证明 $\Leftarrow$：是显然的. 因为每个主理想整环均是唯一因子分解整区.

$\Rightarrow$：设 R 不是主理想整环，则 R 中存在非主理想. 将这个非主理想分解成有限个素理想的乘积，可知至少有其中一个素理想因子不是主理想(反证法). 因此，R 中必存在不是主理想的素理

想 P. 考虑集合 $S=\{R$ 的理想 $I \mid IP$ 为主理想$\}$, 由引理 2 知道 S 是非空的, 从而有极大元 M. 令 $PM=(\alpha)$, $\alpha\in R$, 则 α 必是环 R 中的不可约元素. 这是因为: 如果 $\alpha=\beta\gamma$, β, $\gamma\in R$, 则 $P\mid(\alpha)=(\beta)(\gamma)$, 从而 $P\mid(\beta)$或者 $P\mid(\gamma)$. 于是(β)或者(γ)必有形式 JP, 其中 J 为 R 中理想, 于是 $J\in S$. 又由于 $JP\mid PM$, 从而 $J\mid M$, 即 $J\supseteq M$. 但是 M 为 S 中的极大元, 因此 $J=M$. 从而 $(\beta)=(\alpha)$或者$(\gamma)=(\alpha)$, 即 β 和 γ 当中必有一个与 α 相结合, 因此 α 是不可约元素. 另一方面, 显然 $P\supsetneqq(\alpha)$. 又由于 $R\neq P$, 从而又有 $M\supsetneqq(\alpha)$. 于是有 $\delta\in P-(\alpha)$, $\varepsilon\in M-(\alpha)$. 由于 $(\alpha)=MP\supseteq(\delta)(\varepsilon)=(\delta\varepsilon)$, 从而 $\alpha\mid\delta\varepsilon$. 但是 $\alpha\nmid\delta$, $\alpha\nmid\varepsilon$. 这对于唯一因子分解整环 R 中的不可约元素 α 是不可能的. 这一矛盾表明 R 必为主理想整环. ▌

最后我们再给出一个技术性结果:

引理 8 设 I 是 Dedekind 整环 R 中的理想, 则对于每个 $0\neq\alpha\in I$, 均存在 $\beta\in I$, 使得 $I=(\alpha,\beta)$. 换句话说, Dedekind 整环中每个理想均是二元生成的, 并且其中的一个非零元素可以在 I 中任取.

证明 我们只需在 R 中找一个元素 β 使得 $I=(\alpha)+(\beta)$ 即可, 因为这时自然 $\beta\in I$. 令 $I=P_1^{n_1}P_2^{n_2}\cdots P_r^{n_r}$ $(n_i\geqslant 1)$, 其中 $P_1,\cdots,P_r$ 为 R 中不同的素理想. 由于 $\alpha\in I$, 即 $I\mid(\alpha)$, 从而可设 $(\alpha)=P_1^{f_1}\cdots P_r^{f_r}Q_1\cdots Q_s$, 其中 $Q_j\neq P_i$ 均为 R 的素理想, $n_i\leqslant f_i\in\mathbb{Z}$ $(i=1,\cdots,r;\ j=1,\cdots,s)$, $s\geqslant 0$. 根据我们在引理 5 前面对于最大公因子所作的说明, 可知我们只需取 $\beta\in\bigcap_{i=1}^{r}(P_i^{n_i}-P_i^{n_i+1})\cap\left(\bigcap_{j=1}^{s}(R-Q_j)\right)$ 即可. 而这是可以作到的: 因为 $P_i^{n_i}\supsetneqq P_i^{n_i+1}$, 从而可取 $\beta_i\in P_i^{n_i}-P_i^{n_i+1}$ $(1\leqslant i\leqslant r)$. 然后由中国剩余定理(附录 B, (3))求 $\beta\in R$, 使得

$$\beta\equiv\beta_i\ (\operatorname{mod} P_i^{n_i+1})\quad(1\leqslant i\leqslant r),$$
$$\beta\equiv 1\ (\operatorname{mod} Q_j)\quad(1\leqslant j\leqslant s),$$

则这个 β 即为所求. ▌

1.2 整数环 O_K 是 Dedekind 整环

定理 2 数域 K 的整数环 O_K 是 Dedekind 整环.

证明 O_K 显然是整环. 我们来依次验证 Dedekind 整环定义中的三个条件对于 O_K 是成立的.

(1) 我们在第一章中证明了, O_K 的加法群是有限生成自由 Abel 群. 而每个理想 I 的加法群均是 O_K 的加法子群. 由 Abel 群结构定理(附录 B, (1))可知 I 的加法群也是有限生成的. 即 $I=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$, 于是更有 $I=R\alpha_1+\cdots+R\alpha_n$. 从而 I 作为 R 的理想也是有限生成的, 即 O_K 是诺特整环.

(2) 设 P 是 O_K 中的非零素理想. 取 $0\neq\alpha\in P$, 令 $m=N_{K/Q}(\alpha)\in\mathbb{Z}-\{0\}$. 由于 m/α 是 α 的一些共轭元素之积, 从而 m/α 是整数, 但是 $m/\alpha\in K$, 所以 $m/\alpha\in O_K$. 于是 $m=\alpha\cdot m/\alpha\in P$. 即 $(m)\subseteq P$. 设 $\{\omega_1, \cdots, \omega_n\}$ 为 O_K 的一组整基, 即 $O_K=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$, $n=[K:Q]$. 则

$$\begin{aligned}O_K/mO_K&=(\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n)/\mathbb{Z}m\omega_1\oplus\cdots\oplus\mathbb{Z}m\omega_n\\&\cong\mathbb{Z}/m\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m\mathbb{Z}\quad(n\text{ 个}).\end{aligned}$$

由环的同构定理知道 $O_K/P\cong(O_K/mO_K)/(P/mO_K)$, 从而 $|O_K/P|\leqslant|O_K/mO_K|=m^n$. 即 O_K/P 是有限环. 由于 P 是素理想, 从而 O_K/P 为有限整区, 熟知它必是域. 这就反过来推出 P 为极大理想. 于是环 O_K 中每个非零素理想均是极大理想.

(3) 设 $\alpha\in K$, $f(x)=x^m+c_1x^{m-1}+\cdots+c_m\in O_K[x]$, $f(\alpha)=0$. 由于 $c_1, \cdots, c_m\in O_K$, 可知 O_K 的子环 $R=\mathbb{Z}[c_1, \cdots, c_m]$ 的加法群是有限生成的, 即 $R=\mathbb{Z}\gamma_1+\cdots+\mathbb{Z}\gamma_s$. 由 $f(\alpha)=0$ 可知每个 $\alpha^r(r\geqslant1)$ 均可表示成 $1, \alpha, \cdots, \alpha^{m-1}$ 的 R-线性组合. 于是

$$\begin{aligned}\mathbb{Z}[c_1, \cdots, c_m, \alpha]=R[\alpha]&=R\cdot1+R\alpha+\cdots+R\alpha^{m-1}\\&=\mathbb{Z}\gamma_1+\cdots+\mathbb{Z}\gamma_s+\mathbb{Z}\alpha\gamma_1+\cdots+\mathbb{Z}\alpha\gamma_s+\cdots\\&\quad+\mathbb{Z}\alpha^{m-1}\gamma_1+\cdots+\mathbb{Z}\alpha^{m-1}\gamma_s.\end{aligned}$$

即环 $\mathbb{Z}[c_1, \cdots, c_m, \alpha]$ 的加法群也是有限生成的. 根据第一章定理 8 的(3), 可知 α 是整数, 从而 $\alpha\in O_K$. 这就证明了 O_K 有整闭性

质。 ∎

系 整数环 O_K 的每个非零理想均可(不计次序)唯一地表示成有限个素理想的乘积. ∎

例 考虑虚二次域 $K=\mathbb{Q}(\sqrt{-5})$. 我们从第一章已经知道 $O_K=\mathbb{Z}[\sqrt{-5}]$. 在 O_K 中主理想(2)和(3)都不是素理想, 这是因为

$$(2,\ 1+\sqrt{-5})^2=(2\cdot 2,\ 2\cdot(1+\sqrt{-5}),\ (1+\sqrt{-5})^2)$$
$$=(4,\ 2(1+\sqrt{-5}),\ -4+2\sqrt{-5})=(2);$$
$$(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$$
$$=(9,\ 3+3\sqrt{-5},\ 3-3\sqrt{-5},\ 6)=(3).$$

理想 $(2,\ 1+\sqrt{-5})$ 是素理想, 这是由于商环 $\mathbb{Z}[\sqrt{-5}]/(2,\ 1+\sqrt{-5})$ 是由两个元素构成的整环(验证!). 同样可证 $(3,\ 1+\sqrt{-5})$ 和 $(3,\ 1-\sqrt{-5})$ 也都是 $\mathbb{Z}[\sqrt{-5}]$ 中的素理想. 于是(2)是素理想 $(2,\ 1+\sqrt{-5})$ 的平方, 而理想(3)是两个(不同)素理想 $(3,\ 1+\sqrt{-5})$ 和 $(3,\ 1-\sqrt{-5})$ 的乘积.

读者多半在抽象代数课程中学过, $\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环, 因为元素 6 有两种分解式:

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}),$$

而 2, 3, $1\pm\sqrt{-5}$ 均是不可约元素, 并且 2 与 $1\pm\sqrt{-5}$ 不相伴. 将上述等式改成理想的等式, 就有

$$(6)=(2)\cdot(3)=(1+\sqrt{-5})(1-\sqrt{-5}).$$

验证: $(1+\sqrt{-5})=(2,\ 1+\sqrt{-5})(3,\ 1+\sqrt{-5})$, $(1-\sqrt{-5})=(2,\ 1-\sqrt{-5})(3, 1-\sqrt{-5})$, $(2, 1+\sqrt{-5})=(2,\ 1-\sqrt{-5})$. 从而由元素 6 的两个不同的分解式给出理想(6)的同一个素理想分解式:

$$(6)=(2,\ 1+\sqrt{-5})^2(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5}).$$

在上面例子中我们还看到另一种现象, 即一个素数 p(它生成 $\mathbb{Z}$ 的素理想(p))在整数环 O_K 中生成的理想 $pO_K=(p)$ 可能不再是 O_K 中的素理想. 但是在 Dedekind 整环 O_K 中, 理想 pO_K 应当是 O_K 中一些素理想的乘积. 这就产生了一个很自然的问题: pO_K 是如

何地分解成一些素理想的乘积？更一般地，设 L/K 是数域的扩张，显然 $O_L \supseteq O_K$. 从而 O_K 中的素理想 $\mathfrak{p}$ 是 O_L 的一个子集合. 人们要问：$\mathfrak{p}$ 在 O_L 中生成的理想 $\mathfrak{p}O_L$ 是如何地分解成 O_L 中一些素理想的乘积？这是代数数论的基本问题之一. 本章从第4节起，几乎全是致力于研究这一问题.

1.3 分式理想，理想的范

设 K 为数域. 我们以 $I^\circ(K)$ 表示整数环 O_K 的全部非零理想所构成的集合. 它对于理想的乘法显然是一个带1交换半群，其幺元素就是 $(1)=O_K$. 而由引理5我们知道半群 $I^\circ(K)$ 满足消去律，即如果 $A, B, C \in I^\circ(K)$ 并且 $AC=BC$，则 $A=B$. 大家知道，每个具有消去律的带1交换半群均可嵌到一个交换群 G 之中(就象将非负有理整数加法半群在引进负数之后嵌到有理整数加法群中那样). 构作群 G 的办法通常是形式化的. 但是对于 $I^\circ(K)$ 的情形我们可以不用形式化程序，因为我们可以把 $I^\circ(K)$ 所扩充成的交换群中每个元素赋以更具体的意义，这就是"分式理想".

定义4 数域 K 中的子集合 $I \supsetneqq (0)$ 叫作是 K 中的分式理想，如果存在 $0 \neq \mu \in O_K$，使得 μI 是 O_K 中的理想. 我们以 $I(K)$ 表示 K 中全体分式理想所组成的集合.

例如，O_K 中每个理想均是分式理想(取 $\mu=1$). 有时为明确起见，我们将 O_K 中理想称作是 K 的**整理想**. 于是，$I^\circ(K) \subseteq I(K)$. 又比如，对于每个元素 $0 \neq \alpha \in K$，$(\alpha)=\alpha O_K$ 是分式理想. 这是由于 α 可以表为两个整数之商：$\alpha=\beta/\gamma$, $\beta, \gamma \in O_K$, $\gamma \neq 0$，而 $\gamma(\alpha)=(\beta)$ 为整理想. 我们把由一个元素 $\alpha \in K-\{0\}$ 生成的分式理想 $(\alpha)=\alpha O_K$ 叫作是**主分式理想**.

对于 K 中两个分式理想 A 和 B，定义

$$AB=\left\{\sum_{i=1}^{n} a_i b_i \,\middle|\, a_i \in A,\ b_i \in B,\ n \geqslant 1\right\}. \qquad (*)$$

当 A 和 B 均为整理想时，这就是通常的理想乘积的定义. 而对于

一般的情形，由于 $A=\frac{1}{\alpha}A'$，$B=\frac{1}{\beta}B'$，其中 $\alpha, \beta\in O_K-\{0\}$，$A'$ 和 B' 为整理想，从而 $AB=\frac{1}{\alpha\beta}A'B'$ 也是分式理想．于是，由(*)式定义的乘法是分式理想集合 $I(K)$ 中的运算．

定理 3 分式理想集合 $I(K)$ 对于上面定义的乘积运算是自由 Abel 群．并且每个分式理想 I 均可唯一地表示成两个互素的整理想的商：$I=A/B=AB^{-1}$，其中 $A, B\in I^{\circ}(K)$，$(A, B)=1$．从而 I 也可唯一地表示成 $I=\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}$，其中 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 是 O_K 中不同的素理想，而 $a_i\in\mathbb{Z}-\{0\}$．

证明 为证 $I(K)$ 是群，我们只需证每个分式理想 I 均可逆即可．根据定义 $I=\frac{1}{\mu}A$，其中 $\mu\in O_K-\{0\}$，$A\in I^{\circ}(K)$．由引理 5 知道存在 $B\in I^{\circ}(K)$，使得 $AB=(\alpha)$，$\alpha\in O_K-\{0\}$．于是 $IB=(\alpha/\mu)$，从而 $I\left(\frac{\mu}{\alpha}B\right)=(1)=O_K$，即分式理想 $\frac{\mu}{\alpha}B$ 是 I 的逆，从而 $I(K)$ 为群并且由乘法的定义(*)可知它是 Abel 群．

将公式 $I=A/(\mu)$ 内的分子分母同时除以整理想 A 和 (μ) 的最大公因子，即可将分式理想 I 表成两个互素的整理想之商．由素理想分解式不难证明这种表达方式的唯一性，同时也得到定理 3 中最后一个表达方式． ∎

引理 9 n 次数域 K 中每个分式理想的加法群均是秩 n 的自由 Abel 群．

证明 我们先证这对整理想成立．设 I 是 O_K 的(整)理想，则 I 的加法群是秩 n 自由 Abel 群 O_K 的子群．由 Abel 群基本定理(附录 B，(1))可知 I 的加法群是秩 $\leqslant n$ 的自由 Abel 群．我们只需再证 I 的秩是 n，这只要在 I 中能找到 $\mathbb{Z}$-线性无关的 n 个元素即可．为此设 $\{\omega_1, \cdots, \omega_n\}$ 是 O_K 的一组整基，任取 $0\neq\alpha\in I$，令 $t=N_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}-\{0\}$，则 $t/\alpha\in K$．但是 t/α 是 α 的一些共轭元素的乘积，从而 t/α 为整数，于是 $t/\alpha\in O_K$，因此 $t=t/\alpha\cdot\alpha\in I$．从而 $t\omega_1, \cdots, t\omega_n$ 均属于 I，但是这 n 个数显然是 $\mathbb{Z}$-线性无关

的，这就证明了加法群 I 是秩 n 的自由 Abel 群。

现在设 I 是分式理想，则 $I=\frac{1}{\mu}A$，$\mu\in O_K-\{0\}$，A 为整理想。我们已经证明了 $A=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$，于是 $I=\mathbb{Z}\alpha_1/\mu\oplus\cdots\oplus\mathbb{Z}\alpha_n/\mu$，即每个分式理想 I 的加法群均是秩 n 的自由 Abel 群。 ∎

注记 当 $I=\mathbb{Z}\beta_1\oplus\cdots\oplus\mathbb{Z}\beta_n(\beta_i\in K-\{0\})$ 时，我们把 $\{\beta_1,\cdots,\beta_n\}$ 叫作是分式理想 I 的一组 $\mathbb{Z}$-基。不难看出，分式理想 I 的不同 $\mathbb{Z}$-基之间的变换方阵是行列式为 ±1 的 n 阶 $\mathbb{Z}$-阵。

本节的最后我们谈谈如何用一个数量粗略地衡量一个分式理想的"大小"。先从整理想谈起。我们有一个最"大"的整理想 O_K 作为标准，每个非零整理想 A 均是 O_K 的子集合。设 $\{\omega_1,\cdots,\omega_n\}$ 是 O_K 的一组 $\mathbb{Z}$-基（即整基），$\{\alpha_1,\cdots,\alpha_n\}$ 是 A 的一组 $\mathbb{Z}$-基（引理 9），则 $\alpha_i\in O_K$，从而是 $\{\omega_1,\cdots,\omega_n\}$ 的 $\mathbb{Z}$-线性组合。于是

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=T\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix},T=(t_{ij}),\ t_{ij}\in\mathbb{Z},\ \det T\neq0$$

（$\det T$ 表示方阵 T 的行列式）。如果 $\{\omega_1',\cdots,\omega_n'\}$ 和 $\{\alpha_1',\cdots,\alpha_n'\}$ 分别是 O_K 和 A 的另一组 $\mathbb{Z}$-基，则

$$\begin{pmatrix}\alpha_1'\\ \vdots\\ \alpha_n'\end{pmatrix}=M\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},\quad\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}=N\begin{pmatrix}\omega_1'\\ \vdots\\ \omega_n'\end{pmatrix}.$$

其中 M 和 N 均为 n 阶 $\mathbb{Z}$-方阵，并且 $\det M=\pm1$，$\det N=\pm1$，而

$$\begin{pmatrix}\alpha_1'\\ \vdots\\ \alpha_n'\end{pmatrix}=MTN\begin{pmatrix}\omega_1'\\ \vdots\\ \omega_n'\end{pmatrix},$$

由于 $|\det(MTN)|=|\det T|$（其中 $|\ \ |$ 表示绝对值），这就表明正整数 $|\det T|$ 与 O_K 和 A 的 $\mathbb{Z}$-基选取是无关的，即它是理想 A 本身的不变量，我们称它是**整理想 A 的范**，表示成 $N_K(A)=N_{K/\mathbb{Q}}(A)$。

引理 10 设 A 为数域 K 中的非零整理想,则 $N_K(A)=|O_K/A|$.

证明 按照 Abel 群基本定理(附录 B, (1)), 我们可以取 O_K 的一组整基$\{\omega_1, \cdots, \omega_n\}$, 使得 $O_K=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$, $A=\mathbb{Z}a_1\omega_1\oplus\cdots\oplus\mathbb{Z}a_n\omega_n$, $a_i\in\mathbb{Z}$, 这时

$$\begin{pmatrix} a_1\omega_1 \\ \vdots \\ a_n\omega_n \end{pmatrix}=\begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

从而由理想范的定义可知 $N_K(A)=|a_1a_2\cdots a_n|$. 另一方面,

$$\begin{aligned} O_K/A &=(\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n)/(\mathbb{Z}a_1\omega_1\oplus\cdots\oplus\mathbb{Z}a_n\omega_n) \\ &\cong\mathbb{Z}\omega_1/\mathbb{Z}a_1\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n/\mathbb{Z}a_n\omega_n \\ &\cong\mathbb{Z}/a_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/a_n\mathbb{Z}. \end{aligned}$$

于是 $|O_K/A|=\prod_{i=1}^{n}|\mathbb{Z}/a_i\mathbb{Z}|=|a_1\cdots a_n|=N_K(A)$. ▮

注记 由公式 $N_K(A)=|O_K/A|$ 可以看出, $N_K(A)$愈大则有限环 O_K/A 中元素愈多,从而 A 在 O_K 中的分布愈稀疏. 因此,在某种程度上 $N_K(A)$衡量了理想 A 的大小.

整理想的范有以下的基本性质.

定理 4 设 A 和 B 是域 K 中的整理想, $A=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$, 其中 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 是 O_K 中不同的素理想, $e_i\geqslant1$, 则

(1) $N_K(A)=N_K(\mathfrak{p}_1)^{e_1}\cdots N_K(\mathfrak{p}_r)^{e_r}$;

(2) $N_K(AB)=N_K(A)N_K(B)$;

(3) 设$\{\alpha_1, \cdots, \alpha_n\}$是 A 的一组 $\mathbb{Z}$-基,则

$$d_K(\alpha_1, \cdots, \alpha_n)=N(A)^2d(K);$$

(4) 若 $A=(\alpha)(\alpha\in O_K)$为主理想,则 $N_K(A)=|N_{K/\mathbb{Q}}(\alpha)|$.

证明

(1) 由于理想 $\mathfrak{p}_1^{e_1}, \cdots, \mathfrak{p}_r^{e_r}$ 是彼此互素的,根据中国剩余定理我们有 $O_K/A\cong O_K/\mathfrak{p}_1^{e_1}\oplus\cdots\oplus O_K/\mathfrak{p}_r^{e_r}$, 于是由引理 10 得

$$N_K(A)=|O_K/A|=\prod_{i=1}^{r}|O_K/\mathfrak{p}_i^{e_i}|=\prod_{i=1}^{r}N_K(\mathfrak{p}_i^{e_i}).$$

我们只需再证 $N_K(\mathfrak{p}_i^{a_i})=N_K(\mathfrak{p}_i)^{a_i}$ 即可。为此，对 O_K 中每个素理想 $\mathfrak{p}$ 和 $k\geqslant 1$，由于 $\mathfrak{p}^k\supsetneqq\mathfrak{p}^{k+1}$，因此可取 $\alpha\in\mathfrak{p}^k-\mathfrak{p}^{k+1}$. 作映射

φ: $O_K\to(\alpha O_K+\mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}$, $\varphi(x)=\alpha x+\mathfrak{p}^{k+1}\ (x\in O_K)$，这显然是环的满同态。由 α 的取法可知 $(\alpha)=\mathfrak{p}^kA'$, $(A',\ \mathfrak{p})=1$. 从而 $\alpha O_K+\mathfrak{p}^{k+1}=(\mathfrak{p}^kA',\ \mathfrak{p}^{k+1})=\mathfrak{p}^k$，即 φ 的象为 $\mathfrak{p}^k/\mathfrak{p}^{k+1}$. 另一方面，对于每个 $x\in O_K$，则

$$x\in \operatorname{Ker}\varphi\Leftrightarrow(\alpha x)\subseteq\mathfrak{p}^{k+1}\Leftrightarrow\mathfrak{p}^{k+1}\mid(\alpha x)=\mathfrak{p}^k\cdot A'\cdot(x)$$
$$\Leftrightarrow\mathfrak{p}\mid(x)\Leftrightarrow x\in\mathfrak{p}.$$

这就表明 $\operatorname{Ker}\varphi=\mathfrak{p}$. 因此由环的同构定理我们有环的同构 $O_K/\mathfrak{p}\cong\mathfrak{p}^k/\mathfrak{p}^{k+1}(k\geqslant 1)$. 于是

$$N_K(\mathfrak{p}^r)=|O_K/\mathfrak{p}^r|=|O_K/\mathfrak{p}|\cdot|\mathfrak{p}/\mathfrak{p}^2|\cdots|\mathfrak{p}^{r-1}/\mathfrak{p}^r|$$
$$=|O_K/\mathfrak{p}|^r=N_K(\mathfrak{p})^r,$$

这就完全证明了(1).

(2) 由(1)和 A, B 的素理想分解式立即推得.

(3) 设 $\{\omega_1,\ \cdots,\ \omega_n\}$ 是 O_K 的一组整基, $\{\alpha_1,\ \cdots,\ \alpha_n\}$ 是 A 的一组 $\mathbb{Z}$-基，则

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=M\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

由定义 $N_K(A)=|\det M|$. 设 $\sigma_1,\ \cdots,\ \sigma_n$ 是数域 K 到 $\mathbb{C}$ 中的 n 个嵌入, $n=[K:\mathbb{Q}]$. 由于 M 是 $\mathbb{Z}$-阵，从而将上式作用 σ_i 给出

$$\begin{pmatrix}\sigma_i(\alpha_1)\\ \vdots\\ \sigma_i(\alpha_n)\end{pmatrix}=M\begin{pmatrix}\sigma_i(\omega_1)\\ \vdots\\ \sigma_i(\omega_n)\end{pmatrix},$$

从而有矩阵等式: $(\sigma_i(\alpha_j))=M(\sigma_i(\omega_j))$，于是

$$d_K(\alpha_1,\ \cdots,\ \alpha_n)=\det(\sigma_i(\alpha_j))^2=(\det M)^2(\det(\sigma_i(\omega_j))^2)$$
$$=N_K(A)^2d_K(\omega_1,\ \cdots,\ \omega_n)=N_K(A)^2d(K).$$

(4) 若 $A=(\alpha)$, $\alpha\in O_K-\{0\}$，则 $\{\alpha\omega_1,\ \cdots,\ \alpha\omega_n\}$ 是 A 的一组 $\mathbb{Z}$-基，从而由(3)即知 $d_K(\alpha\omega_1,\ \cdots,\ \alpha\omega_n)=N_K(A)^2d(K)$. 但是

$$d_K(\alpha\omega_1,\ \cdots,\ \alpha\omega_n)=\det(\sigma_i(\alpha\omega_j))^2=\det(\sigma_i(\alpha)\sigma_i(\omega_j))^2$$

$$=\left(\prod_{i=1}^{n}\sigma_i(\alpha)\right)^2\cdot\det(\sigma_i(\omega_j))^2$$
$$=(N_{K/\mathbb{Q}}(\alpha))^2\cdot d(K).$$

于是 $N_K(A)=|N_{K/\mathbb{Q}}(\alpha)|$. ▌

现在不难看出应当如何定义分式理想的范：K 中每个分式理想 I 均可表成两个整理想的商：$I=A/B$. 令 $N_K(I)=N_K(A)/N_K(B)\in\mathbb{Q}$. 如果 I 表成另外两个整理想的商：$I=A'/B'$，则 $AB'=A'B$. 由定理 4 可知 $N_K(A)/N_K(B)=N_K(A')/N_K(B')$，这表明 $N_K(I)$ 与将 I 表成两个整理想之商的方式无关，我们将如此定义的 $N_K(I)\in\mathbb{Q}$ 叫作是**分式理想 I 的范**. 由定理 4 不难把整理想范的诸性质推广到分式理想上：

定理 4' 设 A 和 B 是数域 K 的两个分式理想，则

(1) $N_K(AB)=N_K(A)N_K(B)$.

(2) 如果 $\{\alpha_1,\cdots,\alpha_n\}$ 是 A 的一组 $\mathbb{Z}$-基，则 $d_K(\alpha_1,\cdots,\alpha_n)=N_K(A)^2d(K)$.

(3) 如果 $A=(\alpha)=\alpha O_K(\alpha\in K-\{0\})$ 是主分式理想，则 $N_K(A)=N_{K/\mathbb{Q}}(\alpha)$. ▌

习　题

1. 设 I 是整环 R 的理想. 则 R 为诺特整环 $\Leftrightarrow I$ 和 R/I 均为诺特整环.
2. 设 A 和 B 是 Dedekind 整环 R 中两个理想，$A=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$，$B=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_r^{f_r}$，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 是 R 中不同的素理想，而 $e_i, f_i\geqslant 0$，求证：
   (a) $A|B\Leftrightarrow e_i\leqslant f_i\quad(1\leqslant i\leqslant r)$；
   (b) $A\cap B=\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_r^{t_r}$，$t_i=\max(e_i, f_i)\quad(1\leqslant i\leqslant r)$；
   $A+B=\mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}$，$m_i=\min(e_i, f_i)\quad(1\leqslant i\leqslant r)$.
3. 设 A 为数域 K 的分式理想，求证 $A^{-1}=\{\alpha\in K|\alpha A\subseteq O_K\}$.
4. 求证 O_K 为主理想整环的充要条件是数域 K 中每个分式理想均是主分式理想.
5. 证明 $R=\{f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Q}[x]|0\leqslant n\in\mathbb{Z}, a_0\in\mathbb{Z}\}$ 不是诺特整环.
6. 设 A 和 B 是数域 K 的两个整理想.

(a) 求证：若 $A|B$，则 $N_K(A)|N_K(B)$。试问反过来是否成立？

(b) 如果 $N_K(A)$ 为素数，求证 A 必为 O_K 的素理想。试问反过来是否成立？

7. 设 A 是数域 K 的整理想，$A=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ 为 A 的素理想分解式，以 $(O_K/A)^\times$ 表示有限环 O_K/A 的单位群（即乘法可逆元全体组成的乘法群），令 $\varphi(A)=|(O_K/A)^\times|$。求证：

(a) $\varphi(\mathfrak{p}_i^{e_i})=N_K(\mathfrak{p}_i)^{e_i-1}(N_K(\mathfrak{p}_i)-1)$；

(b) $\varphi(A)=N_K(A)\cdot\prod\limits_{\mathfrak{p}|A}\left(1-\dfrac{1}{N_K(\mathfrak{p})}\right)$.

8. 设 $K=\mathbb{Q}(\alpha)$，$\alpha^3=\alpha+1$。求证：

(a) $O_K=\mathbb{Z}[\alpha]$；

(b) $23O_K=\mathfrak{p}_1^2\mathfrak{p}_2$，其中 $\mathfrak{p}_1=(23,\ \alpha-10)$，$\mathfrak{p}_2=(23,\ \alpha-3)$；

(c) $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 是 O_K 中不同的素理想；

(d) $N_K(\mathfrak{p}_1)=N_K(\mathfrak{p}_2)=23$。

9. 试问二次域 $\mathbb{Q}(\sqrt{10})$ 中的整理想 $(2,\ \sqrt{10})$ 是否为主理想？

10. (a) 设 A 是数域 K 中的整理想，$N_K(A)=g$，求证 $g\in A$；

(b) 对于每个正整数 g，求证 K 中满足 $N_K(A)=g$ 的整理想 A 只有有限多个。

11. (a) 求出域 $\mathbb{Q}(\sqrt{-1})$ 中范为 1, 2, 3, 4, 5 的全部整理想；

(b) 在域 $K=\mathbb{Q}(\sqrt{-1})$ 中求 $2O_K$, $3O_K$, $4O_K$, $5O_K$ 的素理想分解式。

（提示：$O_K=\mathbb{Z}[\sqrt{-1}]$ 是主理想整环。）

12. 设 $\mathfrak{p}$ 为数域 K 的素理想，A 和 B 是 K 中两个整理想。以 $\nu_\mathfrak{p}(A)(\geqslant 0)$ 表示 A 的素因子分解式中 $\mathfrak{p}$ 的指数（若 $\mathfrak{p}$ 在分解式中不出现，则 $\nu_\mathfrak{p}(A)=0$）。求证：$\nu_\mathfrak{p}(AB)=\nu_\mathfrak{p}(A)+\nu_\mathfrak{p}(B)$；$\nu_\mathfrak{p}(A+B)=\min(\nu_\mathfrak{p}(A),\nu_\mathfrak{p}(B))$，$\nu_\mathfrak{p}(A\cap B)=\max(\nu_\mathfrak{p}(A),\ \nu_\mathfrak{p}(B))$。

13. 设 $\mathfrak{p}$ 为数域 K 的素理想，对于 $0\neq a\in O_K$，定义 $\nu_\mathfrak{p}(a)=\nu_\mathfrak{p}(aO_K)$。并且令 $\nu_\mathfrak{p}(0)=+\infty$。同时对 $n\in\mathbb{Z}$，规定

$n+(+\infty)=(+\infty)+(+\infty)=(+\infty)\cdot n=(+\infty)\cdot(+\infty)=+\infty$。

求证当 a, $b\in O_K$ 时，

(a) $\nu_\mathfrak{p}(ab)=\nu_\mathfrak{p}(a)\nu_\mathfrak{p}(b)$，$\nu_\mathfrak{p}(a+b)\geqslant\min(\nu_\mathfrak{p}(a),\nu_\mathfrak{p}(b))$；

(b) 如果 $\nu_\mathfrak{p}(a)\neq\nu_\mathfrak{p}(b)$，则 $\nu_\mathfrak{p}(a+b)=\min(\nu_\mathfrak{p}(a),\nu_\mathfrak{p}(b))$；

(c) 试问当 $\nu_\mathfrak{p}(a)=\nu_\mathfrak{p}(b)$ 时，$\nu_\mathfrak{p}(a+b)=\min(\nu_\mathfrak{p}(a),\ \nu_\mathfrak{p}(b))$ 是否成立？

14. 设 $\mathfrak{p}$ 为数域 K 的素理想，a_1, $\cdots$, $a_n\in O_K$，$a_1+a_2+\cdots+a_n=0$，令 $m=\min\{\nu_\mathfrak{p}(a_i)|1\leqslant i\leqslant n\}$。求证至少存在两个不同的下标 i 和 j，使得

$v_{\mathfrak{p}}(a_i)=v_{\mathfrak{p}}(a_j)=m$.

15. 设 A 是 O_K 的理想，$\alpha, \beta\in O_K$，则 $\alpha x\equiv\beta(\mathrm{mod}\ A)$有解 $x\in O_K$ 的充要条件是$(\alpha O_K,\ A)\,|\,\beta O_K$. 并且在这个条件成立的时候，此同余方程模 $A/(\alpha O_K,\ A)$有唯一解(即：若 x_1 和 $x_2\in O_K$ 均是此同余方程的解，则 $x_1\equiv x_2(\mathrm{mod}A/(\alpha O_K,\ A))$).

§2 分歧指数，剩余类域次数和分裂次数

2.1 e, f, g

现在我们开始研究数域中素理想分解的基本问题. 设 L/K 是数域的扩张. $\mathfrak{a}$ 是 O_K 的一个(整)理想. 基本问题是：O_L 中的理想 $\mathfrak{a}O_L$ 如何分解成 O_L 中素理想的乘积？由于每个理想 $\mathfrak{a}$ 均是 O_K 中一些素理想的乘积，因此我们只要对 O_K 中每个素理想 $\mathfrak{p}$ 弄清 $\mathfrak{p}O_L$ 在 O_L 中的素理想分解式就可以了.

对于 O_K 中每个素理想 $\mathfrak{p}$，显然 $\mathfrak{p}O_L\subsetneqq O_L$. 从而 $\mathfrak{p}O_L$ 在域 L 上分解成

$$\mathfrak{p}O_L=\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},$$

其中 $g\geqslant1$, $\mathfrak{P}_1$, $\cdots$, $\mathfrak{P}_g$ 是 L 中不同的素理想，而 $e_i\geqslant1(1\leqslant i\leqslant g)$. 对于每个 $\mathfrak{P}_i$，我们有 $\mathfrak{P}_i\,|\,\mathfrak{p}O_L$，这也常常简写成 $\mathfrak{P}_i\,|\,\mathfrak{p}$，并且称 O_L 中素理想 $\mathfrak{P}_i$ 是 O_K 中素理想 $\mathfrak{p}$ 的因子(即指是 O_L 中理想 $\mathfrak{p}O_L$ 的因子). 这就首先遇到一个问题：如何判别 O_L 中一个素理想 $\mathfrak{P}$ 是 $\mathfrak{p}$ 的因子？

引理 11 设 L/K 是数域的扩张，$\mathfrak{P}$ 为 O_L 的素理想，则

(1) $\mathfrak{P}\cap O_K$ 为 O_K 的素理想，并且 $\mathfrak{P}\cap O_K=\mathfrak{p}\Leftrightarrow\mathfrak{P}\,|\,\mathfrak{p}$;

(2) 若 $\mathfrak{P}\cap O_K=\mathfrak{p}$，则 $O_K/\mathfrak{p}$ 和 $O_L/\mathfrak{P}$ 均是有限域，并且前者可看成是后者的子域.

证明 (1) 容易验证 $\mathfrak{P}\cap O_K$ 是 O_K 的理想. 进而，若 $a, b\in O_K$, $ab\in\mathfrak{P}\cap O_K$，则 $ab\in\mathfrak{P}$. 由于 $\mathfrak{P}$ 为 O_L 中的素理想，并且 $a,b\in O_L$，从而 $a\in\mathfrak{P}$ 或者 $b\in\mathfrak{P}$. 于是 $a\in\mathfrak{P}\cap O_K$ 或者 $b\in\mathfrak{P}\cap O_K$. 这就证明了 $\mathfrak{P}\cap O_K$ 是 O_K 的素理想.

若$\mathfrak{P}\cap O_K=\mathfrak{p}$，则$\mathfrak{P}\supseteq\mathfrak{p}$，从而$\mathfrak{P}\supseteq\mathfrak{p}O_L$，于是$\mathfrak{P}|\mathfrak{p}O_L$，即$\mathfrak{P}|\mathfrak{p}$. 反之，若$\mathfrak{p}$为$O_K$中的素理想并且$\mathfrak{P}|\mathfrak{p}$，则$\mathfrak{P}|\mathfrak{p}O_L$，于是$\mathfrak{P}\supseteq\mathfrak{p}O_L\supseteq\mathfrak{p}$，从而$\mathfrak{P}\cap O_K\supseteq\mathfrak{p}\cap O_K=\mathfrak{p}$. 但是$\mathfrak{P}\cap O_K$和$\mathfrak{p}$均为$O_K$的素理想，从而均为$O_K$的极大理想，所以必然$\mathfrak{P}\cap O_K=\mathfrak{p}$.

(2) 作映射

$$\varphi: O_K\to O_L/\mathfrak{P},\ \varphi(x)=x+\mathfrak{P}\quad(x\in O_K),$$

易知这是环的同态，而$\mathrm{Ker}\,\varphi=O_K\cap\mathfrak{P}=\mathfrak{p}$. 从而由同态$\varphi$可将环$O_K/\mathfrak{p}$看成是$O_L/\mathfrak{P}$的子环. 我们过去已经证明了$O_K/\mathfrak{p}$和$O_L/\mathfrak{P}$均是有限环(元素个数分别为$N_K(\mathfrak{p})$和$N_L(\mathfrak{P})$). 由于$\mathfrak{p}$和$\mathfrak{P}$分别是$O_K$和$O_L$的极大理想，从而$O_K/\mathfrak{p}$和$O_L/\mathfrak{P}$均是有限域，而前者是后者的子域. ∎

注记 对于每个数域K和每个素数p，显然O_K中均有素理想$\mathfrak{p}$使得$\mathfrak{p}|p$. 另一方面，如果p和p'为不同的素数，而$\mathfrak{p}$和$\mathfrak{p}'$为O_K中素理想，$\mathfrak{p}|p$，$\mathfrak{p}'|p'$，则$\mathfrak{p}\cap\mathbb{Z}=p\neq p'=\mathfrak{p}'\cap\mathbb{Z}$，这就表明$\mathfrak{p}\neq\mathfrak{p}'$. 由于熟知存在无限多个素数$p$，从而对于每个数域$K$，$O_K$中存在着无限多个素理想.

现在可以引进素理想分解的三个最基本参量. 设L/K为数域的扩张. 对于O_K中的素理想$\mathfrak{p}$，$\mathfrak{p}O_L$在O_L中的素理想分解式为：

$$\mathfrak{p}O_L=\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},\ e_i\geqslant1,\ g\geqslant1.$$

$\mathfrak{p}$在O_L中的g个素理想因子$\mathfrak{P}_i(1\leqslant i\leqslant g)$可以用$\mathfrak{P}_i\cap O_K=\mathfrak{p}$来刻划. e_i叫作是$\mathfrak{P}_i$的分歧指数(这个名称来源于代数几何)，表示成$e_i=e(\mathfrak{P}_i/\mathfrak{p})$. 如果$e_i\geqslant2$，称$\mathfrak{P}_i$是(对于扩张$L/K$的)分歧素理想. 否则便称$\mathfrak{P}_i$是不分歧的. 如果$e_1$，…，$e_g$中至少有一个大于2，即$\mathfrak{P}_1$，…，$\mathfrak{P}_g$中至少有一个是分歧的，便称$\mathfrak{p}$(对于扩张$L/K$)是分歧的. 否则，如果$\mathfrak{P}_1$，…，$\mathfrak{P}_g$均是不分歧的，便称$\mathfrak{p}$是不分歧的. 数$g$叫作是分裂次数. 最后，根据引理11可知$O_K/\mathfrak{p}$和$O_L/\mathfrak{P}_i$均是有限域，并且后者是前者的扩域. 这显然是有限(次)扩张. 其扩张次数$[O_L/\mathfrak{P}_i:O_K/\mathfrak{p}]$叫作是$\mathfrak{P}_i$(对于扩张$L/K$)的剩余类域次数，表示成$f(\mathfrak{P}_i/\mathfrak{p})$. 这三个基本参量$g$，$e(\mathfrak{P}_i/\mathfrak{p})$和

$f(\mathfrak{P}_i/\mathfrak{p})(1\leqslant i\leqslant g)$之间有如下关系.

定理 5 设 L/K 是数域的扩张, $n=[L:K]$, $\mathfrak{p}$ 为 O_K 的素理想, $\mathfrak{p}O_L=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$ 为 $\mathfrak{p}O_L$ 在 O_L 中的素理想分解式, $e_i=e(\mathfrak{P}_i/\mathfrak{p})$, $f_i=f(\mathfrak{P}_i/\mathfrak{p})(1\leqslant i\leqslant g)$, 则 $\sum\limits_{i=1}^{g}e_if_i=n$.

证明 由 $\mathfrak{p}O_L$ 的素理想分解式可知 $N_L(\mathfrak{p}O_L)=\prod\limits_{i=1}^{g}N_L(\mathfrak{P}_i)^{e_i}$, 但是 $N_L(\mathfrak{P}_i)=|O_L/\mathfrak{P}_i|$, 而 $O_L/\mathfrak{P}_i$ 是有限域 $O_K/\mathfrak{p}$ 上的f_i维向量空间, 从而 $N_L(\mathfrak{P}_i)=|O_L/\mathfrak{P}_i|=|O_K/\mathfrak{p}|^{f_i}$, 于是 $N_L(\mathfrak{p}O_L)=\prod\limits_{i=1}^{g}|O_K/\mathfrak{p}|^{e_if_i}=|O_K/\mathfrak{p}|^{\sum\limits_{i=1}^{g}e_if_i}$, 另一方面, 作映射

$$\varphi:\ O_K\to O_L/\mathfrak{p}O_L,\ \varphi(x)=\bar{x}=x+\mathfrak{p}O_L\quad(x\in O_K),$$

则 φ 是环同态, 并且 $\operatorname{Ker}\varphi=O_K\cap\mathfrak{p}O_L=\mathfrak{p}$(为什么?), 从而有限域 $O_K/\mathfrak{p}$ 可看成是有限环 $O_L/\mathfrak{p}O_L$ 的子域, 于是 $V=O_L/\mathfrak{p}O_L$ 是有限域 $\overline{K}=O_K/\mathfrak{p}$ 上的向量空间. 记这个向量空间的维数为 $\tilde{n}=\dim_{\overline{K}}V$, 则 $N_L(\mathfrak{p}O_L)=|O_L/\mathfrak{p}O_L|=|V|=|\overline{K}|^{\tilde{n}}=|O_K/\mathfrak{p}|^{\tilde{n}}$, 从而 $\tilde{n}=\sum\limits_{i=1}^{g}e_if_i$, 于是我们只需再证明 $\tilde{n}=n$ 即可.

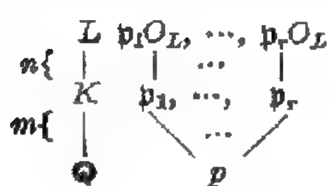
我们先证明 $\tilde{n}\leqslant n$(这等价于 $\sum\limits_{i=1}^{g}e_if_i\leqslant n$). 设 $x_1,\cdots,x_{n+1}$ 是 O_L 中任意 $n+1$ 个元素, 由于$[L:K]=n$, 从而存在不全为0的 $\alpha_1,\cdots,\alpha_{n+1}\in K$, 使得

$$\alpha_1x_1+\cdots+\alpha_{n+1}x_{n+1}=0. \tag{*}$$

必要时将 $\alpha_1,\cdots,\alpha_{n+1}$ 乘以 O_K 中同一个适当的非零整数(例如乘以 $\alpha_1,\cdots,\alpha_{n+1}$ 的"公分母"), 我们可以假设 $\alpha_1,\cdots,\alpha_{n+1}$ 均属于 O_K. 现在令 $\mathfrak{a}=(\alpha_1,\cdots,\alpha_{n+1})$, 这是 O_K 中的理想, 于是有整理想 $\mathfrak{b}$, 使得 $\mathfrak{a}\mathfrak{b}=(\alpha)\not\subset(\alpha)\mathfrak{p}$, $\alpha\in O_K$, 从而存在 $\beta\in\mathfrak{b}$, 使得 $\beta\mathfrak{a}\not\subset(\alpha)\mathfrak{p}$. 因此: (i) $(\beta/\alpha)\mathfrak{a}=\beta\cdot\mathfrak{b}^{-1}\subseteq O_K$. 由此可知$(\beta/\alpha)\cdot\alpha_i\in O_K(1\leqslant i\leqslant n+1)$; (ii) $(\beta/\alpha)\mathfrak{a}\not\subset\mathfrak{p}$. 由此可知, 至少有一个 i 使得$(\beta/\alpha)\cdot\alpha_i\notin\mathfrak{p}$. 换句话说, 如果令 $\gamma_i=(\beta/\alpha)\cdot\alpha_i$, 则 $\gamma_i\in O_K(1\leqslant i\leqslant n+1)$,并且至少有一个 i, 使得 $\gamma_i\notin\mathfrak{p}$, 即在 $\overline{K}=O_K/\mathfrak{p}$中$\bar{\gamma}_i\neq\bar{0}$. 现在将(*)式诸项乘以 β/α, 即得到 $\gamma_1x_1+\cdots+\gamma_{n+1}x_{n+1}=0$. 然后转到商环中, 则为

$\bar{\gamma}_1\bar{x}_1+\cdots+\bar{\gamma}_{n+1}\bar{x}_{n+1}=\bar{0}$，并且 $\bar{\gamma}_1, \cdots, \bar{\gamma}_{n+1}$ 不全为 $\bar{0}$. 这就表明 $V=O_L/\mathfrak{p}O_L$ 中任意 $n+1$ 个元素 $\bar{x}_1, \cdots, \bar{x}_{n+1}$ 在 $\bar{K}=O_K/\mathfrak{p}$ 上都是线性相关的，从而 $\tilde{n}=\dim_{\bar{K}}V\leqslant n$.

现在我们进而证明 $\tilde{n}=n$. 当 $K=\mathbb{Q}$ 时证明是容易的. 因为这时 $\mathfrak{p}$ 即为主理想 (p)，p 为素数，而 $O_K/\mathfrak{p}=\mathbb{Z}/(p)$ 为 p 元域. 设 $\{\omega_1, \cdots, \omega_n\}$ 为 O_L 的一组整基，则 $O_L/(p)O_L=(\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n)/(\mathbb{Z}p\omega_1\oplus\cdots\oplus\mathbb{Z}p\omega_n)\cong\mathbb{Z}\omega_1/\mathbb{Z}p\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n/\mathbb{Z}_p\omega_n\cong\mathbb{Z}(p)\oplus\cdots\oplus\mathbb{Z}/(p)$（$n$ 个），因此 $\tilde{n}=n$. 从而对于 $K=\mathbb{Q}$ 这一特殊情形我们也就证明了定理. 现在考虑一般情形：上述证明不能直接用于一般的 K，因为 K 中素理想 $\mathfrak{p}$ 不一定是主理想，而 O_L 在 O_K 上也不一定有相对整基. 但是我们可借助于 $\mathbb{Q}$（如图所示）. 我们知道，$\mathfrak{p}\cap\mathbb{Z}$ 是 $\mathbb{Z}$ 中的素理想，从而 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$，$p$ 为素数，于是 $\mathfrak{p}|p$. 设 $pO_K=\mathfrak{p}_1^{\tilde{e}_1}\cdots\mathfrak{p}_r^{\tilde{e}_r}$ 是理想 pO_K 在 O_K 中的素理想分解式，$\tilde{e}_i=e(\mathfrak{p}_i/p)$，$\tilde{f}_i=f(\mathfrak{p}_i/p)$，则 $\mathfrak{p}$ 为某个 $\mathfrak{p}_i$. 并且上面已经证明了 $\sum_{i=1}^{r}\tilde{e}_i\tilde{f}_i=[K:\mathbb{Q}]=m$，又令 $\bar{K}_i=O_K/\mathfrak{p}_i$，$V_i=O_L/\mathfrak{p}_iO_L$，则 V_i 是域 $\bar{K}_i$ 上的向量空间. 令维数为 $\tilde{n}_i=\dim_{\bar{K}_i}V_i$，我们上面也已经证明了 $\tilde{n}_i\leqslant n(1\leqslant i\leqslant r)$，由于 $pO_L=(\mathfrak{p}_1O_L)^{\tilde{e}_1}\cdots(\mathfrak{p}_rO_L)^{\tilde{e}_r}$，从而



$$|O_L/pO_L|=N_L(pO_L)=\prod_{i=1}^{r}N_L(\mathfrak{p}_iO_L)^{\tilde{e}_i}=\prod_{i=1}^{r}|O_L/\mathfrak{p}_iO_L|^{\tilde{e}_i}$$

$$=\prod_{i=1}^{r}|O_K/\mathfrak{p}_i|^{\tilde{n}_i\tilde{e}_i}=\prod_{i=1}^{r}p^{\tilde{n}_i\tilde{f}_i\tilde{e}_i}.$$

另一方面，我们已经知道 $|O_L/pO_L|=p^{[L:\mathbb{Q}]}=p^{mn}$. 于是

$$mn=\sum_{i=1}^{r}\tilde{n}_i\tilde{f}_i\tilde{e}_i\leqslant\sum_{i=1}^{r}n\tilde{f}_i\tilde{e}_i=n\sum_{i=1}^{r}\tilde{f}_i\tilde{e}_i=nm,$$

从而必然要 $\tilde{n}_i(1\leqslant i\leqslant r)$ 均等于 n 才行. 而 $\tilde{n}$ 是某个 $\tilde{n}_i$，因此 $\tilde{n}=n$，这就完成了定理 5 的证明. ∎

由定理 5 可知，g 的最大值为 $n=[L:K]$. 并且当 $g=n$ 时，e_i 和 f_i 均为 1，即

$$\mathfrak{p}O_L=\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n,\ e(\mathfrak{P}_i/p)=f(\mathfrak{P}_i/p)=1\quad(1\leqslant i\leqslant n),$$

这时我们称 O_K 的素理想 $\mathfrak{p}$ 在 L 中完全分裂. 另一个极端是 $e=n$ 的情形, 此时 $g=1$, 于是 $\mathfrak{p}O_L=\mathfrak{P}^n$(从而 $e(\mathfrak{P}/\mathfrak{p})=n$, $f(\mathfrak{P}/\mathfrak{p})=1$), 这时称 $\mathfrak{p}$ 在 L 中完全分歧. 最后, 若 $\mathfrak{p}O_L=\mathfrak{P}(g=1, e(\mathfrak{P}/\mathfrak{p})=1, f(\mathfrak{P}/\mathfrak{p})=n)$, 则称 $\mathfrak{p}$ 在 L 中是惯性的, 这是因为 O_K 中素理想扩充成 O_L 中理想 $\mathfrak{p}O_L$ 之后, 仍旧是素理想.

定理 6 (传递公式). 设 L/M 和 M/K 均是数域的扩张, $\mathfrak{p}$, $\mathfrak{P}$, P 分别是 O_K, O_M, O_L 的素理想, 并且 $P|\mathfrak{P}|\mathfrak{p}$ (如图). 则

$$\begin{array}{cc} L & P \\ | & | \\ M & \mathfrak{P} \\ | & | \\ K & \mathfrak{p} \end{array}$$

$$e(P|\mathfrak{p})=e(P/\mathfrak{P})\cdot e(\mathfrak{P}/\mathfrak{p}),\ f(P/\mathfrak{p})=f(P/\mathfrak{P})\cdot f(\mathfrak{P}/\mathfrak{p}).$$

证明 由于 $\mathfrak{p}O_M=\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\cdots$, $\mathfrak{P}O_L=P^{e(P/\mathfrak{P})}\cdots$, 从而

$$\mathfrak{p}O_L=(\mathfrak{p}O_M)O_L=(\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\cdots)O_L=(\mathfrak{P}O_L)^{e(\mathfrak{P}/\mathfrak{p})}\cdots=P^{e(P/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})}\cdots$$

另一方面, $\mathfrak{p}O_L=P^{e(P/\mathfrak{p})}\cdots$因此 $e(P/\mathfrak{p})=e(P/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$. 类似地考虑有限域的扩张 $O_K/\mathfrak{p}\subseteq O_M/\mathfrak{P}\subseteq O_L/P$, 即知

$$f(P/\mathfrak{p})=[O_L/P:O_K/\mathfrak{p}]=[O_L/P:O_M/\mathfrak{P}]\cdot[O_M/\mathfrak{P}:O_K/\mathfrak{p}]=f(P/\mathfrak{P})\cdot f(\mathfrak{P}/\mathfrak{p}).\quad ∎$$

2.2 素理想分解和多项式分解

上一小节中我们介绍了三个基本参量 e, f, g 和基本关系 $n=\sum_{i=1}^{g}e_if_i$. 在一般情形下, 这对于决定数值 g, e_i, f_i 是不够的. 给了 O_K 中素理想 $\mathfrak{p}$, 我们希望有办法能够求出 g, e_i, f_i 的数值以及 $\mathfrak{p}$ 在 O_L 中的全部素理想因子 $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$. 在这方面, 下面定理是很有用的.

定理 7 设 L/K 是数域的扩张, $L=K(\alpha)$, $\alpha\in O_L$, $n=[L:K]$. $f(x)=x^n+c_1x^{n-1}+\cdots+c_n\in O_K[x]$ 是整数 α 在 K 上的极小多项式, 则

(a) $O_K[\alpha]$ 是 O_L 的子环, 并且加法商群 $O_L/O_K[\alpha]$ 是有限群;

(b) 设 p 是素数, $\mathfrak{p}$ 为 O_K 的素理想, $\mathfrak{p}|p$. 则 $O_K/\mathfrak{p}$ 是特征 p 的有限域;

(c) 如果 $\mathfrak{p}\nmid|O_L/O_K[\alpha]|$，令 $f(x)$ 在主理想整区 $O_K/\mathfrak{p}[x]$ 中分解成

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_g(x)^{e_g}\quad(\bmod\mathfrak{p}),$$

其中 $p_1(x)$，$\cdots$，$p_g(x)$ 均为 $O_K[x]$ 中的首 1 多项式，并且看作是 $O_K/\mathfrak{p}[x]$ 中的多项式时(即多项式系数看作是域 $O_K/\mathfrak{p}$ 中的元素)为两两不同的不可约多项式，则 $\mathfrak{p}$ 在 O_L 中的分解式为

$$\mathfrak{p}O_L=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g},$$

其中 $\quad\mathfrak{P}_i=(\mathfrak{p},\ p_i(\alpha))$，$e_i=e(\mathfrak{P}_i/\mathfrak{p})$，而 $f(\mathfrak{P}_i/\mathfrak{p})=\deg p_i(x)$ $(1\leqslant i\leqslant g)$.

证明

(a) $O_K[\alpha]$ 显然是 O_L 的子环. 由于加法群 O_L 和 $O_K[\alpha]$ 均是秩 $[L:\mathbb{Q}]$ 的自由 Abel 群，由 Abel 群基本定理不难看出加法商群 $O_L/O_K[\alpha]$ 是有限的;

(b) 由于 $\mathfrak{p}\cap\mathbb{Z}=p$，并且 $O_K/\mathfrak{p}$ 是 p 元域 $\mathbb{Z}/p\mathbb{Z}$ 的扩域，从而 $O_K/\mathfrak{p}$ 是特征 p 的有限域;

(c) 令 $f_i=\deg p_i(x)(1\leqslant i\leqslant g)$. 我们先依次证明以下三件事情:

(i) 对于每个 i，或者 $\mathfrak{P}_i=O_L$，或者 $O_L/\mathfrak{P}_i$ 是 $|O_K/\mathfrak{p}|^{f_i}$ 元域. 这是因为: $p_i(x)$ 在 $O_K/\mathfrak{p}[x]$ 中不可约，从而 $F_i=O_K/\mathfrak{p}[x]/(p_i(x))$ 为域. 自然同态 φ: $O_K[x]\ \varphi\to O_K/\mathfrak{p}[x]/(p_i(x))$ 是满同态，并且 $\operatorname{Ker}\varphi=(\mathfrak{p},\ p_i(x))$，从而有同构 $O_K[x]/(\mathfrak{p},\ p_i(x))\cong O_K/\mathfrak{p}[x]/(p_i(x))=F_i$，从而左边也是域. 因此 $(\mathfrak{p},\ p_i(x))$ 是 $O_K[x]$ 的极大理想. 再作映射 π: $O_K[x]\to O_L/\mathfrak{P}_i$，$\pi(f(x))=f(\alpha)+\mathfrak{P}_i$，这是环同态. 由于 $\mathfrak{P}_i=(\mathfrak{p},\ p_i(\alpha))$，从而 $(\mathfrak{p},\ p_i(x))\subseteq\operatorname{Ker}\pi$，但是 $(\mathfrak{p},\ p_i(x))$ 是 $O_K[x]$ 的极大理想. 因此 $\operatorname{Ker}\pi=(\mathfrak{p},\ p_i(x))$ 或者 $O_K[x]$. 我们再证 π 是满同态，这只要证明 $O_K[\alpha]+\mathfrak{P}_i=O_L$ 即可. 由于 $p\in\mathfrak{p}\subseteq\mathfrak{P}_i$，从而 $pO_L\subseteq\mathfrak{P}_i$，于是只要证明 $O_K[\alpha]+pO_L=O_L$ 即可. 这是由于 $p\nmid|O_L/O_K[\alpha]|$，而 $|O_L/pO_L|=p^{[L:\mathbb{Q}]}$，从而 $|O_L/O_K[\alpha]+pO_L|$ 可除尽 $(|O_L/O_K[\alpha]|,\ |O_L/pO_L|)=1$，因此 $|O_L/O_K[\alpha]+pO_L|=1$，即 $O_L=O_K[\alpha]+pO_L$，从而 π 为满同态，于是 $O_L/\mathfrak{P}_i$ 或

者同构于$O_K[x]/(\mathfrak{p}, P_i(x))\cong F_i$，从而$O_L/\mathfrak{P}_i$为$|O_K/\mathfrak{p}|^f$元域；或者同构于$O_K[x]/O_K[x]$，即$\mathfrak{P}_i=O_L$.

(ii) 当$i\neq j$时，$(\mathfrak{P}_i, \mathfrak{P}_j)=1$. 这是由于$p_i(x)$和$p_j(x)$是$O_K/\mathfrak{p}[x]$中不同的不可约多项式，而$O_K/\mathfrak{p}[x]$为主理想整环，从而有$h(x), k(x)\in O_K/\mathfrak{p}[x]$，使得$hp_i+kp_j\equiv 1 \pmod{\mathfrak{p}}$. 代入$x=\alpha$即知$p_i(\alpha)h(\alpha)+p_j(\alpha)k(\alpha)\equiv 1 \pmod{\mathfrak{p}O_L}$，于是$1\in(\mathfrak{p}, p_i(\alpha), p_j(\alpha))=(\mathfrak{P}_i, \mathfrak{P}_j)$.

(iii) $\mathfrak{p}O_L|\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$. 这是因为：令$\gamma_i=p_i(\alpha)$，则$\mathfrak{P}_i=(\mathfrak{p}, \gamma_i)$，由(ii)知当$i\neq j$时，$(\mathfrak{p}, \gamma_i, \gamma_j)=1$. 令$\mathfrak{a}=(\mathfrak{p}, \gamma_1^{e_1}\cdots\gamma_g^{e_g})$，则$\mathfrak{P}_1\mathfrak{P}_2=(\mathfrak{p}, \gamma_1)(\mathfrak{p}, \gamma_2)=(\mathfrak{p}^2, \mathfrak{p}\gamma_1, \mathfrak{p}\gamma_2, \gamma_1\gamma_2)=(\mathfrak{p}(\mathfrak{p}, \gamma_1, \gamma_2), \gamma_1\gamma_2)=(\mathfrak{p}, \gamma_1\gamma_2)$，$\mathfrak{P}_1^2=(\mathfrak{p}, \gamma_1)^2=(\mathfrak{p}^2, \mathfrak{p}\gamma_1, \gamma_1^2)\subseteq(\mathfrak{p}, \gamma_1^2)$. 由此归纳下去，即知$\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}\subseteq(\mathfrak{p}, \gamma_1^{e_1}\cdots\gamma_g^{e_g})=\mathfrak{a}$，只需再证$\mathfrak{a}=\mathfrak{p}O_L$即可. 为证此将$x=\alpha$代入$f(x)\equiv p_1(x)^{e_1}\cdots p_g(x)^{e_g} \pmod{\mathfrak{p}}$，便得到$\gamma_1^{e_1}\cdots\gamma_g^{e_g}\equiv f(\alpha)=0 \pmod{\mathfrak{p}O_L}$，即$\gamma_1^{e_1}\cdots\gamma_g^{e_g}\in\mathfrak{p}O_L$，从而$\mathfrak{a}=(\mathfrak{p}, \gamma_1^{e_1}\cdots\gamma_g^{e_g})=\mathfrak{p}O_L$.

现在我们证明(c)：由(i)我们不妨假设$\mathfrak{P}_1, \cdots, \mathfrak{P}_s$均不为$O_L$，而$\mathfrak{P}_{s+1}=\cdots=\mathfrak{P}_g=O_L$，则$\mathfrak{P}_i(1\leqslant i\leqslant s)$均为$O_L$的素理想，并且$\mathfrak{P}_i\supseteq\mathfrak{p}$. $f_i(\mathfrak{P}_i/\mathfrak{p})=[O_L/\mathfrak{P}_i: O_K/\mathfrak{p}]=f_i(1\leqslant i\leqslant s)$. 由(ii)知$\mathfrak{P}_1, \cdots, \mathfrak{P}_s$两两相异，由(iii)知$\mathfrak{p}O_L|\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}$，于是$\mathfrak{p}O_L=\mathfrak{P}_1^{d_1}\cdots\mathfrak{P}_s^{d_s}$，$d_i\leqslant e_i(1\leqslant i\leqslant s)$. 由定理5即知$n=d_1f_1+\cdots+d_sf_s\leqslant e_1f_1+\cdots+e_gf_g$. 但是由$f(x)\equiv p_1(x)^{e_1}\cdots p_g(x)^{e_g} \pmod{\mathfrak{p}}$可知有$e_1f_1+\cdots+e_gf_g=n$. 从而必然$s=g$并且$e_i=d_i(1\leqslant i\leqslant g)$. 这就完成了定理7的证明. ▌

注记 特别若存在$\alpha\in O_L$，使得$O_L=O_K[\alpha]$，即$\{1, \alpha, \cdots, \alpha^{n-1}\}$形成扩张$L/K$的相对整基时，则对于$O_K$的每个素理想$\mathfrak{p}$，均可利用定理7得到$\mathfrak{p}O_L$的分解式. 这就是$\{1, \alpha, \cdots, \alpha^{n-1}\}$型(相对)整基的一个好处.

例 易证$f(x)=x^3+x+1$是$\mathbb{Q}[x]$中不可约多项式. 设ω是它的一个根，则$K=\mathbb{Q}(\omega)$为三次域. 由于$d_K(1, \omega, \omega^2)=d_K(f)=-31$没有平方因子，从而$\{1, \omega, \omega^2\}$为$O_K$的一组整基，即

$O_K=\mathbb{Z}[\omega]$. 于是对于每个素数 p, 我们均可利用定理 7 给出 pO_K 的素理想分解式. 例如:

对于 $p=2$, $f(x)=x^3+x+1$ 在 $\mathbb{F}_2[x]$ 中仍不可约 (因为 $f(x)$ 在 $\mathbb{F}_2$ 中无根). 从而 $2O_K$ 为 O_K 中素理想, 即 2 在 K 中是惯性的.

对于 $p=3$, $f(x)$ 在 $\mathbb{F}_3[x]$ 中分解为 $f(x)=(x-1)(x^2+x-1)$, 而 (x^2+x-1) 在 $\mathbb{F}_3[x]$ 中不可约. 于是 $3O_K=\mathfrak{p}_1\mathfrak{p}_2$, 其中 $\mathfrak{p}_1=(3, \omega-1)$, 和 $\mathfrak{p}_2=(3, \omega^2+\omega-1)$ 为 O_K 中两个不同的素理想, 并且剩余类域次数分别为 $f_1=1$ 和 $f_2=2$. 于是 $N_K(\mathfrak{p}_1)=3$, $N_K(\mathfrak{p}_2)=9$, 而 3 在 K 中不分歧.

对于 $p=31$, $x^3+x+1\equiv(x-3)(x-14)^2 \pmod{31}$. 从而 $31O_K=\mathfrak{p}_1\mathfrak{p}_2^2$, $\mathfrak{p}_1=(31, \omega-3)$, $\mathfrak{p}_2=(31, \omega-14)$, $N_K(\mathfrak{p}_1)=N_K(\mathfrak{p}_2)=31$. $\mathfrak{P}_2$ 是分歧素理想, 从而 31 在 K 中分歧.

2.3 应用: 素数在二次域中的分解, 二平方和定理

利用定理 7, 我们可以完全决定素数 p 在二次域中的素理想分解. 设 $K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}$, 无平方因子. 我们已经知道 $O_K=\mathbb{Z}\oplus\mathbb{Z}\omega$, 其中

$$\omega=\begin{cases}\sqrt{d}, & \text{当 } d\equiv 2, 3 \pmod 4 \text{ 时},\\ \frac{1}{2}(1+\sqrt{d}), & \text{当 } d\equiv 1 \pmod 4 \text{ 时},\end{cases} \quad \text{而 } d(K)=\begin{cases}4d\\ d.\end{cases}$$

我们还需要 Legendre 符号$\left(\frac{d}{p}\right)$, 它定义为:

设 p 为素数, $p\nmid d$, 如果 d 为模 p 的二次剩余(即有 $a\in\mathbb{Z}$, 使得 $d\equiv a^2 \pmod p$), 定义$\left(\frac{d}{p}\right)=1$; 如果 d 为模的 p 非二次剩余, 就定义$\left(\frac{d}{p}\right)=-1$.

定理 8 设 $K=\mathbb{Q}(\sqrt{d})$, p 为素数, $N=N_K$.

(a) 如果 $p\mid d(K)$, 则 $pO_K=\mathfrak{p}^2$, $N(\mathfrak{p})=p$, 即 p 在 K 中分歧;

(b) 若 $p\geqslant 3$, 并且 $p\nmid d(K)$, 则当$\left(\frac{d}{p}\right)=1$ 时, $pO_K=\mathfrak{p}_1\mathfrak{p}_2$,

$\mathfrak{p}_1\neq\mathfrak{p}_2$, $N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=p$, 即 p 在 K 中完全分裂; 而当$\left(\frac{d}{p}\right)=-1$ 时, $pO_K=\mathfrak{p}$, $N(\mathfrak{p})=p^2$, 即 p 在 K 中惯性;

(c) 若 $p=2$ 并且 $p\nmid d(K)$, 则必然 $d\equiv1 \pmod 4$. 如果 $d\equiv 1 \pmod 8$, 则 2 在 K 中完全分裂; 如果 $d\equiv5 \pmod 8$, 则 2 在 K 中惯性.

证明 由于 O_K 有形如 $\{1,\ \omega\}$ 的整基, 从而对于每个素数 p 均可用定理 7.

(i) 设 $d\equiv2,\ 3 \pmod 4$. 这时 $\omega=\sqrt{d}$, 它的极小多项式为 x^2-d, $d(K)=4d$.

设 $p\geqslant3$. 当 $p\nmid d$ 时, 如果$\left(\frac{d}{p}\right)=1$, 即有 $a\in\mathbb{Z}$, 使得 $d\equiv a^2 \pmod p$, 则 $x^2-d\equiv(x-a)(x+a) \pmod p$. 由 $p\nmid d$ 可知 $a\not\equiv -a \pmod p$. 即 $x-a$ 和 $x+a$ 是 $\mathbb{Z}/p\mathbb{Z}[x]$中不同的多项式. 因此 $pO_K=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1=(p,\ \sqrt{d}-a)\neq(p,\ \sqrt{d}+a)=\mathfrak{p}_2$, $N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=p$. 如果$\left(\frac{d}{p}\right)=-1$, 则 x^2-d 为 $\bmod p$ 不可约多项式, 从而 $pO_K=\mathfrak{p}$, $N(\mathfrak{p})=p^2$. 如果 $p|d$, 则 $x^2-d\equiv x^2 \pmod p$, 因此 $pO_K=\mathfrak{p}^2$, $\mathfrak{p}=(p,\ \sqrt{d})$, $N(\mathfrak{p})=p$.

再设 $p=2$. 当 $d\equiv2 \pmod 4$ 时, $x^2-d\equiv x^2 \pmod 2$, 从而 $2O_K=\mathfrak{p}^2$, $\mathfrak{p}=(2,\ \sqrt{d})$, $N(\mathfrak{p})=2$. 如果 $d\equiv3 \pmod 4$, 则 $x^2-d\equiv(x+1)^2 \pmod 2$, 从而 $2O_K=\mathfrak{p}^2$, $\mathfrak{p}=(2,\ \sqrt{d}+1)$, $N(\mathfrak{p})=2$. 因此不论如何, 2 在 K 中总是分歧的.

(ii) 现在设 $d\equiv1 \pmod 4$. 这时 $\omega=\frac{1}{2}(1+\sqrt{d})$, 它的极小多项式为 $x^2-x-\frac{1}{4}(d-1)\in\mathbb{Z}[x]$, $d(K)=d$.

先设 $p\geqslant3$. 这时我们仍用 $\mathbb{Z}[\sqrt{d}]$. 因为 $|O_K/\mathbb{Z}[\sqrt{d}]|=|\mathbb{Z}[w]/\mathbb{Z}[\sqrt{d}]|=2$, 于是 $p\nmid|O_K/\mathbb{Z}[\sqrt{d}]|$. 从而利用定理 7, 可知其结论与 $d\equiv2,\ 3 \pmod 4$ 的情形完全相同.

再设 $p=2$. 当 $d\equiv1 \pmod 8$ 时, $x^2-x-\frac{1}{4}(d-1)\equiv x(x-1)$

(mod 2). 于是 $2O_K=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1=(2,\omega)\neq(2,\omega-1)=\mathfrak{p}_2$, $N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=2$; 而当 $d\equiv5 \pmod 8$ 时, $x^2-x-\frac{1}{4}(d-1)\equiv x^2+x+1 \pmod 2$ 是不可约的. 于是 2 在 K 中惯性. 这就完成了定理 8 的证明. ∎

作为定理 8 的应用，我们来谈谈高斯当年如何用二次域的素理想分解来解决"二平方和"问题. 高斯的代数工具是虚二次域 $\mathbb{Q}(i)$ 和它的整数环 $\mathbb{Z}[i]$, $i=\sqrt{-1}$. (后人将 $\mathbb{Q}(i)$ 和 $\mathbb{Z}[i]$ 分别称作高斯数域和高斯整数环.) 大家在抽象代数中已经学过, $\mathbb{Z}[i]$ 是主理想整环(或者参见本书第三章), 从而 $\mathbb{Z}[i]$ 中每个理想均有形式 $\mathfrak{a}=(a+bi)$, $a, b\in\mathbb{Z}$. 于是 $N(\mathfrak{a})=N(a+ib)=(a+ib)(a-ib)=a^2+b^2$ 正好是两个有理整数的平方和. 换句话说, 我们证明了下面的(a):

(a) $n\in\mathbb{Z}$ 可表为两个有理整数的平方和 $\Leftrightarrow$ n 是 $\mathbb{Z}[i]$ 中某个(主)理想的范;

(b) 若 n 和 m 均可表成两个有理整数的平方和, 则 nm 亦然. (这是因为 $n=N(\alpha)$, $m=N(\beta)$, α, $\beta\in\mathbb{Z}[i]$, 则 $nm=N(\alpha\beta)$.)

有了这些简单的准备, 我们就可以证明:

定理 9(高斯, 二平方和定理)　设 n 为正整数, $n=m^2n_0$, $m\in\mathbb{Z}$, n_0 是 n 的无平方因子部分, 则: n 是两个有理整数的平方和 $\Leftrightarrow$ n_0 没有素因子 $p\equiv3 \pmod 4$.

证明　$\Leftarrow$: 如果 $n_0=1$, 则 $n=m^2+0^2$. 如果 $n_0\geqslant2$, 则 $n_0=p_1\cdots p_s$, $p_1, \cdots, p_s$ 为 $s\geqslant1$ 个不同的素数, 并且 $p_i=2$ 或者 $p_i\equiv1 \pmod 4$. 若 $p_i=2$, 则 $p_i=1^2+1^2$. 若 $p_i\equiv1 \pmod 4$, 则 $\left(\frac{-1}{p_i}\right)=1$. 由定理 8 知 p_i 在 $\mathbb{Z}[i]$ 中完全分裂. 即 $p_i=\mathfrak{p}_1\mathfrak{p}_2$, $N(\mathfrak{p}_1)=p_i$. 于是由前面的(a)知 p_i 可表成二平方和. 再由(b)即知 $n_0=p_1\cdots p_s$ 从而 $n=m^2n$ 均可表为二个整数的平方和.

$\Rightarrow$: 假设 n 可表成二平方和, 则 $\mathbb{Z}[i]$ 中有理想 $\mathfrak{a}$ 使得

$N(\mathfrak{a})=n$. 如果存在素数 $p\equiv 3(\bmod 4)$，使得 $p\mid n_0$，则 $n=m^2n_0$ 中的素因子分解式中包含 p 的奇次幂. 但是另一方面，$\left(\frac{-1}{p}\right)=-1$，从而由定理 8 可知 $pO_K=\mathfrak{p}$ 为 $O_K=\mathbb{Z}[i]$ 中的素理想. $N(\mathfrak{p})=p^2$，并且 $\mathfrak{p}$ 是 $\mathbb{Z}[i]$ 中唯一的素理想使得 $p\mid N(\mathfrak{p})$，因此，若令 $\mathfrak{a}$ 的素理想分解式中 $\mathfrak{p}$ 的个数为 $t\geqslant 0$, $t\in\mathbb{Z}$, 则 $n=N(\mathfrak{a})=p^{2t}\cdots$, 即 n 中包含偶数个 p, 这就导致矛盾. 从而 n_0 中不存在素因子 $p\equiv 3(\bmod)$. ▮

2.4 判别式定理

在这一小节里我们要解决这样一个问题: 如何判别素数 p 在数域 K 中是否分歧? 对于二次域 K 的情形, 从定理 8 可以看出, p 在 K 中分歧的充要条件是 $p\mid d(K)$. Dedekind 成功地证明了, 这个结论对于任意数域都是对的. 为了证明这个结果, 我们需要一些准备工作.

定义 5 如果 B 是域 F 上的有限维向量空间，并且 B 本身又是环，同时对任意 $\xi, \eta\in B$, $a\in F$，均有

$$a(\xi\eta)=(a\xi)\eta=\xi(a\eta), \tag{*}$$

我们就称 B 是域 F 上的代数.

例如，设 L/K 为数域的扩张，则 L 显然是 K 上的代数. 又如，设 $\mathfrak{p}$ 为数域 K 的素理想，$\mathfrak{p}\mid p$（p 是有理素数），则 $p\in\mathfrak{p}^e\cap\mathbb{Z}$，$e=e(\mathfrak{p}\mid p)$，从而 $p\mathbb{Z}\subseteq\mathfrak{p}^e\cap\mathbb{Z}$. 但是 $1\notin\mathfrak{p}^e$，于是 $p\mathbb{Z}\subseteq\mathfrak{p}^e\cap\mathbb{Z}\subsetneq\mathbb{Z}$. 由于 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想，因此必然 $\mathfrak{p}^e\cap\mathbb{Z}=p\mathbb{Z}$. 作自然同态 φ: $\mathbb{Z}\to O_K/\mathfrak{p}^e$，核为 $\operatorname{Ker}\varphi=\mathfrak{p}^e\cap\mathbb{Z}=p\mathbb{Z}$，从而 p 元域 $\mathbb{Z}/p\mathbb{Z}$ 可看成是有限环 $O_K/\mathfrak{p}^e$ 的子域. 于是环 $O_K/\mathfrak{p}^e$ 为域 $\mathbb{Z}/p\mathbb{Z}$ 上的有限维向量空间. 而定义中的(*)式也显然成立. 从而 $O_K/\mathfrak{p}^e$ 为 $\mathbb{Z}/p\mathbb{Z}$ 上的代数.

设环 B 是域 F 上的代数. $\{\xi_1, \cdots, \xi_n\}$ 是 F 上向量空间 B 的一组基. 对于每个 $\xi\in B$，我们有

$$\xi(\xi_1, \cdots, \xi_n)=(\xi\xi_1, \cdots, \xi\xi_n)=(\xi_1, \cdots, \xi_n)A(\xi), \tag{1}$$

其中 $A(\xi)$ 是元素属于域 F 的 n 阶方阵. 如果改用向量空间 B 的另一组基，则方阵 $A(\xi)$ 改成另一个与之相似的方阵，从而方阵的迹 $T_rA(\xi)$ 与基 $(\xi_1, \cdots, \xi_n)$ 的选取无关，叫作是元素 ξ 对于 B/F 的迹，表示成 $T_{B/F}(\xi)$. 当 B/F 是数域的扩张时，$T_{B/F}(\xi)$ 与我们在第一章中定义的迹是一致的(第1节习题13).

对于 B 中 n 个元素 $\xi_1, \cdots, \xi_n$，我们也定义它们的判别式为

$$d_{B/F}(\xi_1, \cdots, \xi_n)=\det(T_{B/F}(\xi_i\xi_j))\ (\in F).$$

引理 12 设 B_1, B_2 均为域 F 上的代数，则环的直和 $B=B_1\oplus B_2$ 也是 F 上的代数. 此外，若 $\{\xi_1, \cdots, \xi_n\}$ 和 $\{\eta_1, \cdots, \eta_m\}$ 分别是 F 上向量空间 B_1 和 B_2 的基，则 $\{\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_m\}$ 是 $B_1\oplus B_2$ 的一组基，并且

$$\begin{aligned}&d_{B/F}(\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_m)\\&\quad=d_{B_1/F}(\xi_1, \cdots, \xi_n)\cdot d_{B_2/F}(\eta_1, \cdots, \eta_m).\end{aligned}\tag{2}$$

证明 直接验证即可(注意 $\xi_i\eta_j=0$). ▮

设 K 为数域，有理素数 p 在 O_K 中分解为 $pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$，则由中国剩余定理我们有 $O_K/pO_K\cong O_K/\mathfrak{p}_1^{e_1}\oplus\cdots\oplus O_K/\mathfrak{p}_g^{e_g}$. 我们已经说过，每个 $O_K/\mathfrak{p}_i^{e_i}$ 均是 p 元域 $\mathbb{Z}/p\mathbb{Z}$ 上的代数，从而由引理 12 可知 O_K/pO_K 也是如此.

引理 13

(a) 设 $\{\omega_1, \cdots, \omega_n\}$ 为 O_K 的一组整基，则 $\{\overline{\omega}_1, \cdots, \overline{\omega}_n\}$ 为 $B=O_K/pO_K$ 的一组 $\mathbb{F}_p$-基，其中对 $\lambda\in O_K$，我们以 $\bar{\lambda}$ 表示 λ 的模 pO_K 剩余类，而 $\mathbb{F}_p$ 表示 p 元域;

(b) $\lambda\in O_K$，则 $T_{B/\mathbb{F}_p}(\bar{\lambda})=\overline{T_{K/\mathbb{Q}}(\lambda)}$, $d_{B/\mathbb{F}_p}(\overline{\omega}_1, \cdots, \overline{\omega}_n)=\overline{d(K)}$.

证明

(a) B 中元素均可写成 $\bar{\gamma}$, $\gamma\in O_K$. 由于 $\gamma=\sum_{i=1}^{n}c_i\omega_i\ (c_i\in\mathbb{Z})$，从而 $\bar{\gamma}=\sum_{i=1}^{n}\bar{c}_i\overline{\omega}_i(\bar{c}_i\in\mathbb{F}_p)$. 另一方面，如果 $\sum_{i=1}^{n}\bar{c}_i\overline{\omega}_i=0(\bar{c}_i\in\mathbb{F}_p,\ c_i\in\mathbb{Z})$，则 $\sum_{i=1}^{n}c_i\omega_i\in pO_K$，于是 $\sum_{i=1}^{n}c_i\omega_i=p\left(\sum_{i=1}^{n}d_i\omega_i\right)$, $d_i\in\mathbb{Z}$，从而 $c_i=pd_i(1\leqslant i\leqslant n)$，即 $\bar{c}_i=\bar{0}(1\leqslant i\leqslant n)$. 这就表明 $\{\overline{\omega}_1, \cdots, \overline{\omega}_n\}$ 是 B 的

一组 $\mathbb{F}_p$-基。

(b) 对于 $\lambda\in O_K$. 令 $\lambda(\omega_1, \cdots, \omega_n)=(\omega_1, \cdots, \omega_n)A(\lambda)$, $A(\lambda)=(a_{ij})$, $a_{ij}\in\mathbb{Z}$ mod p 之后为 $\bar{\lambda}(\bar{\omega}_1, \cdots, \bar{\omega}_n)=(\bar{\omega}_1, \cdots, \bar{\omega}_n)\bar{A}(\bar{\lambda})$, $\bar{A}(\bar{\lambda})=(\bar{a}_{ij})$, $\bar{a}_{ij}\in\mathbb{F}_p$, 于是

$$T_{B/\mathbb{F}_p}(\bar{\lambda})=T_r(\bar{A}(\bar{\lambda}))=\overline{T_r(A(\lambda))}=\overline{T_{K/\mathbb{Q}}(\lambda)};$$

$$d_{B/\mathbb{F}_p}(\bar{\omega}_1, \cdots, \bar{\omega}_n)=\det(T_{B/\mathbb{F}_p}(\bar{\omega}_i\bar{\omega}_j))$$
$$=\overline{\det(T_{K/\mathbb{Q}}(\omega_i\omega_j))}=\overline{d(K)}. \quad ∎$$

现在考虑 $\mathbb{F}_p$ 上的代数 $B_i=O_K/\mathfrak{p}_i^{e_i}$. 由于 $|O_K/\mathfrak{p}_i^{e_i}|=N(\mathfrak{p}_i^{e_i})=p^{e_if_i}$, 从而向量空间 B_i 在域 $\mathbb{F}_p$ 上的维数是 e_if_i.

引理 14 设 $\eta_1, \cdots, \eta_{e_if_i}$ 是向量空间 B_i 的一组 $\mathbb{F}_p$-基, 则

$$d_{B_i/\mathbb{F}_p}(\eta_1, \cdots, \eta_{e_if_i})=0\Leftrightarrow e_i\geqslant 2.$$

证明 为符号简单起见, 我们去掉 B_i, e_i, f_i, $\mathfrak{p}_i$ 的下标 i, 对于 $\mu\in O_K$, 以 $\bar{\mu}$ 表示 μ 的模 $\mathfrak{p}^e$ 剩余类.

如果 $e\geqslant 2$, 取 $\pi\in\mathfrak{p}-\mathfrak{p}^2$, 则 $\bar{\pi}\neq\bar{0}$, $\bar{\pi}^e=\bar{0}$. 熟知我们可以取 B_i 的一组 $\mathbb{F}_p$-基 $\{\xi_1, \cdots, \xi_{ef}\}$, 使得 $\xi_1=\bar{\pi}$, 于是 $(\bar{\pi}\xi_j)^e=\bar{0}(1\leqslant j\leqslant ef)$. 考虑

$$(\bar{\pi}\xi_j)(\xi_1, \cdots, \xi_{ef})=(\xi_1, \cdots, \xi_{ef})A(\bar{\pi}\xi_j).$$

从而 $(\bar{0}, \cdots, \bar{0})=(\bar{\pi}\xi_j)^e(\xi_1, \cdots, \xi_{ef})=(\xi_1, \cdots, \xi_{ef})A(\bar{\pi}\xi_j)^e$, 因此 $A(\bar{\pi}\xi_j)^e=0$, 即 $A(\bar{\pi}\xi_j)$ 为幂零方阵. 从而它的全部特征根均为 $\bar{0}$. 于是 $T_{B/\mathbb{F}_p}(\xi_1\xi_j)=T_r(A(\bar{\pi}\xi_j))=\bar{0}(1\leqslant j\leqslant ef)$, 从而方阵 $(T_{B/\mathbb{F}_p}(\xi_i\xi_j))$ 的第一行元素均为 0. 于是 $d_{B/\mathbb{F}_p}(\xi_1, \cdots, \xi_{ef})=\det(T_{B/\mathbb{F}_p}(\xi_i\xi_j))=\bar{0}$. 由于 $d_{B/\mathbb{F}_p}(\eta_1, \cdots, \eta_{ef})$ 与 $d_{B/\mathbb{F}_p}(\xi_1, \cdots, \xi_{ef})$ 相差 $\mathbb{F}_p$ 中一个非零元素的平方, 从而 $d_{B/\mathbb{F}_p}(\eta_1, \cdots, \eta_{ef})=0$.

如果 $e=1$, 则 $B=O_K/\mathfrak{p}$ 为 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ 的 f 次扩域, 即 B 为 p^f 元域. 于是 $B/\mathbb{F}_p$ 为单扩张: $B=\mathbb{F}_p(\bar{\lambda})$, $\bar{\lambda}$ 在 $\mathbb{F}_p$ 上的极小多项式为 $\mathbb{F}_p[x]$ 中不可约 f 次多项式 $f(x)$, $f(x)$ 的全部根为 $\bar{\lambda}$, $\bar{\lambda}^p$, $\cdots$, $\bar{\lambda}^{p^{f-1}}$. 并且 $\bar{1}$, $\bar{\lambda}$, $\cdots$, $\bar{\lambda}^{f-1}$ 是向量空间 B 的一组 $\mathbb{F}_p$-基, 对于 $\bar{\mu}\in B$, 令

$$\bar{\mu}(\bar{1}, \bar{\lambda}, \cdots, \bar{\lambda}^{f-1})=(\bar{1}, \bar{\lambda}, \cdots, \bar{\lambda}^{f-1})A(\bar{\mu}),$$

则 $A(\bar{\mu})$ 为 $\mathbb{F}_p$ 上 f 阶方阵. 易知 $f(A(\bar{\lambda}))=A(f(\bar{\lambda}))=A(0)=$

0. 由于 $f(x)$ 在 $\mathbb{F}_p[x]$ 中不可约，可知 $f(x)$ 就是 $A(\bar{\lambda})$ 的特征多项式，从而 $A(\bar{\lambda})$ 有 n 个不同的特征根 $\bar{\lambda}, \bar{\lambda}^p, \cdots, \bar{\lambda}^{p^{f-1}}$，所以 $A(\bar{\lambda}^j)=A(\bar{\lambda})^j$ 的特征根为 $\bar{\lambda}^j, \bar{\lambda}^{jp}, \cdots, \bar{\lambda}^{j(p^{f-1})}$，因此 $T_{B/\mathbb{F}_p}(\bar{\lambda}^j)=T_r(A(\bar{\lambda}^j))=\sum_{i=0}^{f-1}(\bar{\lambda}^j)^{p^i}$. 于是

$$d_{B/\mathbb{F}_p}(\bar{1}, \bar{\lambda}, \cdots, \bar{\lambda}^{f-1})=\begin{vmatrix} \bar{1} & \bar{\lambda} & \cdots & \bar{\lambda}^{f-1} \\ \bar{1} & \bar{\lambda}^p & \cdots & (\bar{\lambda}^p)^{f-1} \\ \cdots & \cdots & \cdots & \cdots \\ \bar{1} & \bar{\lambda}^{p^{f-1}} & \cdots & (\bar{\lambda}^{p^{f-1}(f-1)}) \end{vmatrix}^2$$

$$=\prod_{0\leqslant j<k\leqslant f-1}(\bar{\lambda}^{p^j}-\bar{\lambda}^{p^k})\neq 0.$$

从而对 B 的任意一组 $\mathbb{F}_p$-基 $\eta_1, \cdots, \eta_f$，也有 $d_{B/\mathbb{F}_p}(\eta_1, \cdots, \eta_f)\neq 0$. ▌

有了上面的准备，不难得到下面的著名结果：

定理 10（Dedekind，判别式定理） 有理素数 p 在数域 K 中分歧的充要条件是 $p|d(K)$.

证明 我们有 $pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$, $O_K/pO_K\cong O_K/\mathfrak{p}_1^{e_1}\oplus\cdots\oplus O_K/\mathfrak{p}_g^{e_g}$. 由于 $\bar{\omega}_1, \cdots, \bar{\omega}_n$ 是 $B=O_K/pO_K$ 的一组 $\mathbb{F}_p$-基，并且 $d_{B/\mathbb{F}_p}(\bar{\omega}_1, \cdots, \bar{\omega}_n)=\overline{d(K)}$，因此 $p|d(K)\Leftrightarrow d_{B/\mathbb{F}_p}(\bar{\omega}_1, \cdots, \bar{\omega}_n)=\bar{0}$.

另一方面，设 $\{\xi_{i1}, \cdots, \xi_{i,e_if_i}\}$ 为 $B_i=O_K/\mathfrak{p}_i^{e_i}$ 的一组 $\mathbb{F}_p$-基. 由引理 12 知道 $\{\xi_{i,j}|1\leqslant i\leqslant g, 1\leqslant j\leqslant e_if_i\}$ 是 B 的一组 $\mathbb{F}_p$-基，并且

$$d_{B/\mathbb{F}_p}(\xi_{i,j}|1\leqslant i\leqslant g, 1\leqslant j\leqslant e_if_i\})=\prod_{i=1}^{g}d_{B_i/\mathbb{F}_p}(\xi_{i,j}|1\leqslant j\leqslant e_if_i\}). \tag{1}$$

于是 $p|d(K)\Leftrightarrow d_{B/\mathbb{F}_p}(\bar{\omega}_1, \cdots, \bar{\omega}_n)=\bar{0}\Leftrightarrow$(1)式左边为 $0\Leftrightarrow$(1)式右边至少有一个因子为 $\bar{0}\Leftrightarrow$ 至少有一个 $e_i\geqslant 2\Leftrightarrow p$ 在 K 中分歧. ▌

由定理 10 立刻推出

系 对于每个数域 K，只有有限多个素数 p 在 K 中分歧. ▌

注记 我们在第三章中要证明，当 $K\neq\mathbb{Q}$ 时，$|d(K)|\geqslant 2$. 这就表明对于每个数域 $K\neq\mathbb{Q}$，至少存在一个素数 p 在 K 中分歧.

例 1 三次域 $K=\mathbb{Q}(\omega)$ $(\omega^3+\omega+1=0)$ 的判别式为 $d(K)$

$=-31$. 从而只有 $p=31$ 在 K 中分歧.

例 2 我们在第一章已经计算出，分圆域 $K=\mathbb{Q}(\zeta)$ $(\zeta=\zeta_{p^n})$ 的判别式是素数 p 的方幂. 所以只有 p 在 K 中分歧. 令 $\mathfrak{p}_k=(1-\zeta^k)O_K$. 由于我们已经算出过 $\prod\limits_{\substack{k=1\\p\nmid k}}^{p^n}(1-\zeta^k)=p$，因此 $pO_K=\prod\limits_{\substack{k=1\\p\nmid k}}^{p^n}(1-\zeta^k)\,O_K=\prod\limits_{\substack{k=1\\p\nmid k}}^{p^n}\mathfrak{p}_k$. 当 $p\nmid k$ 时，令 $k'k\equiv 1\pmod{p^n}$，则 $(1-\zeta^k)/(1-\zeta)=1+\zeta+\cdots+\zeta^{k-1}$ 和 $(1-\zeta)/(1-\zeta^k)=(1-\zeta^{k'k})/(1-\zeta^k)=1+\zeta^k+\zeta^{2k}+\cdots+\zeta^{(k'-1)k}$ 均为 O_K 中整数，从而 $(1-\zeta)$ 和 $1-\zeta^k$ 是相结合的元素，于是 $\mathfrak{p}_k=(1-\zeta^k)O_K=(1-\zeta)O_K=\mathfrak{p}_1$，从而 $pO_K=\mathfrak{p}_1^{\varphi(p^n)}$. 由于 $\varphi(p^n)=[K:\mathbb{Q}]$，这就表明 $\mathfrak{p}_1=(1-\zeta)O_K$ 必然是素理想，并且 p 在 $K=\mathbb{Q}(\zeta)$ 中是完全分歧的.

2.5 应用：纯三次域的整基

设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in\mathbb{Z}[x]$，$p$ 为素数并且 $p\mid a_i$ $(1\leqslant i\leqslant n)$，$p^2\nmid a_n$. 由 Eisenstein 判别法可知 $f(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式，令 ω 是 $f(x)$ 的一个根，则 n 次数域 $K=\mathbb{Q}(\omega)$ 叫作是对于 p 的 **Eisenstein 型数域**，简称作 **(E,p) 型数域**.

引理 15 设 $K=\mathbb{Q}(\omega)$ 为上述的 (E,p) 型数域，则 p 在 K 中完全分歧，并且 $p\nmid|O_K/\mathbb{Z}[\omega]|$.

证明 设 $\mathfrak{p}$ 为 K 中素理想，$\mathfrak{p}\mid p$，$e=e(\mathfrak{p}\mid p)$，则 $1\leqslant e\leqslant n$. 由于 $\omega^n+a_1\omega^{n-1}+\cdots+a_n=0$，并且 $p\mid a_i$ $(1\leqslant i\leqslant n)$，从而 $\omega^n\in\mathfrak{p}$，于是 $\omega\in\mathfrak{p}$. 设 $\omega\in\mathfrak{p}^s-\mathfrak{p}^{s+1}$，则 $s\geqslant 1$. 以 $t_0, t_1, \cdots, t_n$ 分别表示主理想 (ω^n), $(a_1\omega^{n-1})$, $\cdots$, (a_n) 中出现的 $\mathfrak{p}$ 因子的指数，则 $t_0=ns$，$t_1\geqslant e+(n-1)s>e$，$\cdots$，$t_{n-1}\geqslant e+s>e$，$t_n=e$. 由于 $t_0, t_1, \cdots, t_n$ 中的最小值至少在两个 t_i 处达到（第 3 节习题 15），这只可能是 $ns=e$. 但是 $e\leqslant n$，从而只有 $s=1$，$e=n$，即 p 在 K 中完全分歧：$pO_K=\mathfrak{p}^n$.

如果 $p\mid|O_K/\mathbb{Z}[\omega]|$，则加法群 $O_K/\mathbb{Z}[\omega]$ 中有 p 阶元素. 即存在 $\mu\in O_K-\mathbb{Z}[\omega]$，使得 $p\mu=x_0+x_1\omega+\cdots+x_{n-1}\omega^{n-1}$，$x_i\in\mathbb{Z}$. 由于 $pO_K=\mathfrak{p}^n$，$\omega\in\mathfrak{p}-\mathfrak{p}^2$（因为 $s=1$），从而

$$x_0+x_1\omega+\cdots+x_{n-1}\omega^{n-1}=p\mu\in\mathfrak{p}^n\Rightarrow x_0\in\mathfrak{p}\Rightarrow x_0\in\mathfrak{p}\cap\mathbb{Z}=$$
$$p\mathbb{Z}\Rightarrow p\mid x_0\Rightarrow x_0\in\mathfrak{p}^n\Rightarrow x_1\omega\in\mathfrak{p}^2\Rightarrow x_1\in\mathfrak{p}\Rightarrow p\mid x_1\Rightarrow x_1\in\mathfrak{p}^n$$
$$\Rightarrow x_2\omega^2\in\mathfrak{p}^3\Rightarrow x_2\in\mathfrak{p}\Rightarrow p\mid x_2\Rightarrow\cdots\Rightarrow p\mid x_{n-1}.$$

于是 $\mu\in\mathbb{Z}[\omega]$，这与假设 $\mu\notin\mathbb{Z}[\omega]$ 相矛盾，从而 $p\nmid|O_K/\mathbb{Z}[\omega]|$. ▌

例 对于每个素数 p 和 $n\geqslant 2$，$K=\mathbb{Q}(\sqrt[n]{p})$ 为 $(E,\ p)$ 型数域，因为 $\sqrt[n]{p}$ 的极小多项式为 x^n-p，从而 p 在 K 中完全分歧并且 $p\nmid|O_K/\mathbb{Z}[\sqrt[n]{p}]|$.

现在我们来完全决定纯三次域的整基. 所谓纯三次域即指 $K=\mathbb{Q}(\sqrt[3]{m})$，$\sqrt[3]{m}\notin\mathbb{Q}$. 不妨设 $m\in\mathbb{Z}$，$m>0$ 并且 m 没有立方因子. 于是 m 可以唯一地写成 $m=ab^2$，其中 a 和 b 是没有平方因子并且彼此互素的正有理整数. 我们令

$$\alpha=\sqrt[3]{ab^2}=\sqrt[3]{m},\quad \beta=\frac{1}{b}\alpha^2=\sqrt[3]{a^2b},$$

则 $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$，并且 $\{1,\ \alpha,\ \beta\}$ 是域 K 的一组 $\mathbb{Q}$-基，这是因为

$$d_K(1,\ \alpha,\ \beta)=\frac{1}{b^2}d_K(1,\ \alpha,\ \alpha^2)=-27a^2b^2\neq 0.$$

定理 11 设 $K=\mathbb{Q}(\sqrt[3]{m})$，$a$，$b$，$\alpha$，$\beta$ 如上所述.

(1) 若 $a^2\not\equiv b^2\pmod 9$，则 $\{1,\ \alpha,\ \beta\}$ 为 O_K 的一组整基；若 $a^2\equiv b^2\pmod 9$，则 $\{\alpha,\ \beta,\ \gamma=\frac{1}{3}(1+a\alpha+b\beta)\}$ 为 O_K 的一组整基.

(2) $d(K)=\begin{cases}-27a^2b^2, & \text{若 } a^2\not\equiv b^2\pmod 9;\\ -3a^2b^2, & \text{若 } a^2\equiv b^2\pmod 9.\end{cases}$

(3) 如果 $p\mid ab$，则 p 在 K 中完全分歧. 对于 $p=3$，则当 $a^2\not\equiv b^2\pmod 9$ 时 3 在 K 中完全分歧；而当 $a^2\equiv b^2\pmod 9$ 时 $3=\mathfrak{p}_1^2\mathfrak{p}_2$，$\mathfrak{p}_1\neq\mathfrak{p}_2$.

证明 由 $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$ 可知 α 和 β 的极小多项式分别为 $f_1(x)=x^3-ab^2$ 和 $f_2(x)=x^3-a^2b$. 由于 a 没有平方因子并且 $(a,\ b)=1$. 因此对于 a 的每个素因子 p，利用 $f_1(x)$ 可知 K 是 $(E,\ p)$ 型数域. 于是由引理 15 可知 p 在 K 中完全分歧（从而 $p\mid d(K)$）

并且 $p\nmid|O_K/\mathbb{Z}[\alpha]|$. 类似地，用 $f_2(x)$ 可知对于 b 的每个素因子 p' 亦有 $p'|d(K)$, p' 在 K 中完全分歧，并且 $p'\nmid|O_K/\mathbb{Z}[\beta]|$. 这就证明了：对于每个 $p|ab$, p 在 K 中均完全分歧，并且 $ab|d(K)$. 但是 $d_K(1, \alpha, \beta)=-27a^2b^2$，而 $d_K(1, \alpha, \beta)$ 与 $d(K)$ 相差一个平方因子，从而 $d(K)=-3a^2b^2$ 或者 $-27a^2b^2$.

如果 $3|ab$，由上述可知 3 在 K 中完全分歧，并且当 $3|a$ 时 $3\nmid|O_K/\mathbb{Z}[\alpha]|$，而当 $3|b$ 时 $3\nmid|O_K/\mathbb{Z}[\beta]|$. 令 $N=\mathbb{Z}\oplus\mathbb{Z}\alpha\oplus\mathbb{Z}\beta$. 由于 $\alpha^2=b\beta\in N$, $\beta^2=a\alpha\in N$, 从而 $\mathbb{Z}[\alpha]\subseteq N$, $\mathbb{Z}[\beta]\subseteq N$. 于是 $|O_K/N|$ 同时除尽 $|O_K/\mathbb{Z}[\alpha]|$ 和 $|O_K/\mathbb{Z}[\beta]|$. 因此总有 $3\nmid|O_K/N|$. 但是 $d_K(1, \alpha, \beta)=-27a^2b^2=|O_K/N|^2\cdot d(K)$，而 $d(K)=-3a^2b^2$ 或 $-27a^2b^2$. 从而 $|O_K/N|$ 只能为 1 或3，于是必然 $|O_K/N|=1$, 即 $N=O_K$. 这就证明了：当 $3|ab$ 时，$\{1, \alpha, \beta\}$ 是 O_K 的一组整基.

如果 $3\nmid ab$，则 $a^2\equiv b^2\equiv 1 \pmod 3$，即 $3|(a^2-b^2)$. 令 $\mu=\alpha-a\in O_K$，则 $K=\mathbb{Q}(\mu)$，而 μ 的极小多项式为

$$g(x)=(x+a)^3-ab^2=x^3+3ax^2+3a^2x+a(a^2-b^2).$$

如果 $a^2\not\equiv b^2 \pmod 9$，考虑 $g(x)$ 的诸系数可知 K 为 $(E, 3)$ 型数域，从而 3 在 K 中完全分歧，并且 $3\nmid|O_K/\mathbb{Z}[\mu]|=|O_K/\mathbb{Z}[\alpha]|$. 由于 $N\supseteq\mathbb{Z}[\alpha]$，从而与上面一样可证得 $\{1, \alpha, \beta\}$ 是 O_K 的整基，从而对全部 $a^2\not\equiv b^2 \pmod 9$ 的情形，$d(K)=d_K(1, \alpha, \beta)=-27a^2b^2$.

最后设 $3\nmid ab$, $b^2\equiv a^2 \pmod 9$. 我们已经证明了 3 在 K 中分歧(因为 $3|d(K)$). 为了证明 $3=\mathfrak{p}_1^2\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$，只需再证 3 在 K 中不完全分歧即可. 证明用反证法：假如 $3O_K=\mathfrak{p}^3$，由于 $\mu^3+3a\mu^2+3a^2\mu+a(a^2-b^2)=0$, 可知 $3|\mu^3$, 即 $\mu\in\mathfrak{p}$. 令 $\mu\in\mathfrak{p}^s-\mathfrak{p}^{s+1}$，则 $s\geqslant 1$. 如果 $s\geqslant 3$，则 $\mu=3\lambda$, $\lambda\in O_K$. 以 $\mu^{(1)}$, $\mu^{(2)}$, $\mu^{(3)}$ 表示 μ 的 3 个共轭元素，则 $\mu^{(i)}=3\lambda^{(i)}$. 从而 $3a^2=\mu^{(1)}\mu^{(2)}+\mu^{(1)}\mu^{(3)}+\mu^{(2)}\mu^{(3)}=9(\lambda^{(1)}\lambda^{(2)}+\lambda^{(1)}\lambda^{(3)}+\lambda^{(2)}\lambda^{(3)})$, 于是 $3|a^2$. 这与假设 $3\nmid a$ 相矛盾，所以 $1\leqslant s\leqslant 2$. 由于 $\alpha=\mu+a$, 从而

$$\mu^3+3a\alpha\mu+a(a^2-b^2)=\mu^3+3a\mu^2+3a^2\mu+a(a^2-b^2)=0.$$

由于 $3\nmid ab$，从而 $((3),(\alpha))=1$，于是 $\mathfrak{p}\nmid(\alpha)$. 又由于 $9\mid(a^2-b^2)$，从而 a^2-b^2 中素因子 3 的指数 $r\geqslant 2$. 于是上式左边各项中 $\mathfrak{p}$ 的指数分别为 $3s$、$3+s$和 $3r$，它们至少有两个为其最小值(第三章习题 15). 由 $1\leqslant s\leqslant 2$ 可知 $3s\neq 3+s$，由 $r\geqslant 2$ 可知 $3r\neq 3+s$，从而必然 $3s=3r<3+s$. 但是这在 $r\geqslant 2$，$1\leqslant s\leqslant 2$ 时是不可能的. 这一矛盾表明 3 在 K 中不能完全分歧，从而只能是 $3O_K=\mathfrak{p}_1^2\mathfrak{p}_2$，$\mathfrak{p}_1\neq\mathfrak{p}_2$.

于是 $\mu^3\in 3O_K=\mathfrak{p}_1^2\mathfrak{p}_2$，从而 $\mu\in\mathfrak{p}_1\mathfrak{p}_2$，因此 $\mu^2\in\mathfrak{p}_1^2\mathfrak{p}_2^2\subseteq\mathfrak{p}_1^2\mathfrak{p}_2=3O_K$，即 $3\mid\mu^2=\alpha^2-2a\alpha+a^2=(1+a\alpha+b\beta)+(a^2-1-3a\alpha)$，于是 $3\mid(1+a\alpha+b\beta)$. 从而 $\gamma=\frac{1}{3}(1+a\alpha+b\beta)\in O_K$由于 $\gamma\notin N$，从而 $O_K\neq N$，于是 $|O_K/N|=3$. 令 $N'=\mathbb{Z}\alpha\oplus\mathbb{Z}\beta\oplus\mathbb{Z}\gamma$，则 $N\subsetneqq N'\subseteq O_K$，从而 $N'=O_K$. 这就证明了：当 $a^2\equiv b^2\pmod 9$时，α，β，γ 为 O_K 的一组整基，并且 $d(K)=-3a^2b^2$. ∎

习　题

1. (a) 求素数 $p=3, 7, 11, 13$ 在 $K=\mathbb{Q}(\sqrt{-5})$中的素理想分解式；
   (b) 求素数 $p=3, 5, 11, 13$ 在 $K=\mathbb{Q}(\sqrt{7})$中的素理想分解式.
2. 设 $K=\mathbb{Q}(\omega)$，$\omega^3=\omega-1$，求 $p=2, 3, 5$ 在 K 中的素理想分解式. 试问哪些素数在 K 中分歧？
3. 何种正整数 n 可表成 $n=a^2+2b^2$，a、$b\in\mathbb{Z}$？(提示：$\mathbb{Z}[\sqrt{-2}]$为主理想整环.)
4. 设 p 为奇素数，$a\in\mathbb{Z}$，$\sqrt[p]{a}\notin\mathbb{Z}$. 求证 p 在 $K=\mathbb{Q}(\sqrt[p]{a})$中必分歧.
5. (a) 设 L/K 为数域的扩张. 如果数域 K 的某个素理想 $\mathfrak{p}$ 在 L 中不分歧，则它在每个中间域 $M(K\subseteq H\subseteq L)$中也不分歧；
   (b) 将"不分歧"改成"完全分歧"，则上述命题(a)也是对的. 改成"完全分裂"也是如此. 改成"惯性"呢？
6. 设 L/K 和 L'/K 均为数域的扩张. 如果 K 中某个素理想 $\mathfrak{p}$ 在 L 中完全分歧而在 L' 中不分歧，则 $L\cap L'=K$.
7. (Dedekind)　设 $K=\mathbb{Q}(\lambda)$，$\lambda^3-\lambda^2-2\lambda-8=0$. 求证：
   (a) $[K:\mathbb{Q}]=3$；

(b) $\mu=\frac{1}{2}(\lambda^2-\lambda)-1\in O_K$. 并且$\{1, \lambda, \mu\}$是$O_K$的一组整基;

(c) 2 在 K 中完全分裂;

(d) 求 $p=503$ 在 K 中的素理想分解式.

8. 设 K 是(E, p)型 n 次数域. 求证对于每个 $\gamma\in O_K$, 均有 $a\in\mathbb{Z}$, 使得 $N_{K/\mathbb{Q}}(\gamma)\equiv a^n(\bmod p)$.

§3 伽罗华扩域中的素理想分解

如果数域扩张 L/K 是伽罗华扩张, Hilbert 于上世纪末研究了这种扩张中素理想分解的更加精细的结构. 我们在这节中介绍 Hilbert 理论的基本结果. 作为应用, 我们还给出分圆域中素理想分解的完整结果并且在下一节中给出 Kronecker-Weber 定理的一个证明.

3.1 $n=efg$

我们在第 3 节中定义了数域 K 中理想 $\mathfrak{a}$ 的范 $N_{K/\mathbb{Q}}(\mathfrak{a})=|O_K/\mathfrak{a}|$. 现在我们将它加以推广到更一般的情形.

定义 设 L/K 是数域的扩张, $\mathfrak{P}$ 和 $\mathfrak{p}$ 分别是 L 和 K 中的素理想, $\mathfrak{P}|\mathfrak{p}$, $f=f(\mathfrak{P}/\mathfrak{p})$, 定义 $N_{L/K}(\mathfrak{P})=\mathfrak{p}^f$. 更一般地, 对于 L 中每个(分式)理想 $\mathfrak{a}=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$ $(e_i\in\mathbb{Z})$, 定义 $N_{L/K}(\mathfrak{a})=\prod_{i=1}^{r}N_{L/K}(\mathfrak{P}_i)^{e_i}$, 不难证明如此定义的(相对)范有以下简单性质(作为习题 1).

(I) 如果 $\mathfrak{A}$ 和 $\mathfrak{B}$ 均是 L 中的理想, 则 $N_{L/K}(\mathfrak{A}\mathfrak{B})=N_{L/K}(\mathfrak{A})N_{L/K}(\mathfrak{B})$.

(II) 对于 $\alpha\in L^\times$, $N_{L/K}(\alpha O_L)=N_{L/K}(\alpha)O_K$.

(III) 如果 $\mathfrak{a}$ 是 K 中的理想, 则 $N_{L/K}(\mathfrak{a}O_L)=\mathfrak{a}^{[L:K]}$.

(IV) 对于扩张 $K/\mathbb{Q}$ 的情形, 对于 K 中理想 $\mathfrak{a}$ 这里关于 $N_{K/\mathbb{Q}}(\mathfrak{a})$ 的定义与早先的定义 $N_{K/\mathbb{Q}}(\mathfrak{a})=|O_K/\mathfrak{a}|$ 是一致的(但需把数 $m=|O_K/\mathfrak{a}|\in\mathbb{Z}$ 等同于 $\mathbb{Z}$ 中的理想 $(m)=m\mathbb{Z}$).

(V) 设 L/M 和 M/K 均是数域的扩张，则对于 L 中的理想 $\mathfrak{A}$，$N_{L/K}(\mathfrak{A})=N_{M/K}(N_{L/M}(\mathfrak{A}))$。

现在设 L/K 是数域的伽罗华扩张，$G=\mathrm{Gal}(L/K)$是该扩张的伽罗华群. 对于每个整数 $\alpha\in O_L$，α 的每个 K-共轭元素 $\sigma(\alpha)$ $(\sigma\in G)$ 与 α 在 K 上具有同一个极小多项式，从而均是 L 中的整数，即 $\sigma(\alpha)\in O_L$. 于是 $\sigma(O_L)\subseteq O_L$(对每个 $\sigma\in G$)，从而必然 $\sigma(O_L)=O_L(\sigma\in G)$. 类似地，若 $\mathfrak{P}$ 是 O_L 的素理想，则 $\sigma(\mathfrak{P})=\{\sigma(\alpha)|\alpha\in\mathfrak{P}\}$ 也是 O_L 的素理想，称作是 $\mathfrak{P}$ 的 K-共轭理想.

定理 12 设 L/K 是数域的伽罗华扩张，$n=[L:K]$. $G=\mathrm{Gal}(L/K)$. $\mathfrak{p}$ 为 O_K 中的素理想，$\mathfrak{p}$ 在 O_L 中的分解式为

$$\mathfrak{p}O_L=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g},\ f_i=f(\mathfrak{P}_i/\mathfrak{p})\quad(1\leqslant i\leqslant g),$$

则

(a) 群 G 在集合$\{\mathfrak{P}_1,\ \cdots,\ \mathfrak{P}_g\}$上是可迁的，即对于每对 $\mathfrak{P}_i$ 和$\mathfrak{P}_j$，均存在 $\sigma\in G$ 使得 $\sigma(\mathfrak{P}_i)=\mathfrak{P}_j$;

(b) 对于每个 i，$\{\mathfrak{P}_1,\ \cdots,\ \mathfrak{P}_g\}$ 就是 $\mathfrak{P}_i$ 的全部 K-共轭理想;

(c) $e_1=e_2=\cdots=e_g$, $f_1=f_2=\cdots=f_g$. 令 $e=e_i$, $f=f_i(1\leqslant i\leqslant g)$，则 $n=efg$;

(d) 对于 L 中每个理想 $\mathfrak{A}$，均有 $N_{L/K}(\mathfrak{A})O_L=\prod_{\sigma\in G}\sigma(\mathfrak{A})$.

证明 (a) 由于 G 是群，我们只需证明：对于每个 $i(1\leqslant i\leqslant g)$，均存在 $\sigma\in G$ 使得 $\mathfrak{P}_i=\sigma(\mathfrak{P}_1)$. 证明用反证法. 如果 $\mathfrak{P}_i\notin\{\sigma(\mathfrak{P}_1)|\sigma\in G\}$，则由中国剩余定理可知存在 $\alpha\in O_L$，使得 $\alpha\in\mathfrak{P}_i$ 并且 $\alpha\notin\sigma(\mathfrak{P}_1)$对每个 $\sigma\in G$)，于是 $\sigma(\alpha)\notin\mathfrak{P}_1$ (对每个 $\sigma\in G$). 因此 $N_{L/K}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)\notin\mathfrak{P}_1$，但是 $N_{L/K}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)\in\mathfrak{P}_i\cap O_K=\mathfrak{p}\subseteq\mathfrak{P}_1$，这就导致矛盾，从而证明了(a).

(b) 我们只需证明 $\mathfrak{P}_1$ 的 K-共轭理想必然是 $\mathfrak{P}_1,\ \cdots,\ \mathfrak{P}_g$ 当中的一个. 设 $\mathfrak{P}$ 是 $\mathfrak{P}_1$ 的一个 K-共轭理想，则有 $\sigma\in G$ 使得 $\mathfrak{P}=\sigma(\mathfrak{P}_1)$，但是 $\mathfrak{P}_1\cap O_K=\mathfrak{p}$，从而 $\mathfrak{P}\cap O_K=\sigma(\mathfrak{P}_1)\cap\sigma(O_K)=\sigma(\mathfrak{p})=\mathfrak{p}$. 于是 $\mathfrak{P}|\mathfrak{p}$，即 $\mathfrak{P}$ 必为 $\mathfrak{P}_1,\ \cdots,\ \mathfrak{P}_g$ 中的一个.

(c) 对于每个 $i(1\leqslant i\leqslant g)$. 由 (b) 知有 $\sigma\in G$ 使得 $\mathfrak{P}_i=\sigma(\mathfrak{P}_1)$. 于是

$$\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}=\mathfrak{p}O_L=\sigma(\mathfrak{p}O_L)=\sigma(\mathfrak{P}_1)^{e_1}\cdots\sigma(\mathfrak{P}_g)^{e_g}$$
$$=\mathfrak{P}_i^{e_1}\sigma(\mathfrak{P}_2)^{e_2}\cdots\sigma(\mathfrak{P}_g)^{e_g}.$$

当 $i\neq j$ 时, $\mathfrak{P}_i\neq\mathfrak{P}_j$, 从而 $i\geqslant 2$ 时 $\sigma(\mathfrak{P}_i)\neq\sigma(\mathfrak{P}_1)=\mathfrak{P}_i$. 因此由 $\mathfrak{p}O_L$ 的素理想分解式的唯一性, 比较上式两边 $\mathfrak{P}_i$ 的指数, 即知 $e_i=e_1$, 即 $e_1=e_2=\cdots=e_g$. 同样地:

$$f_i=[O_L/\mathfrak{P}_i:O_K/\mathfrak{p}]=[\sigma(O_L)/\sigma(\mathfrak{P}_i):\sigma(O_K)/\sigma(\mathfrak{p})]$$
$$=[O_L/\mathfrak{P}_1:O_K/\mathfrak{p}]=f_1.$$

于是 $f_1=f_2=\cdots=f_g$. 令 $e=e_i$, $f=f_i(1\leqslant i\leqslant g)$, 则 $n=\sum\limits_{i=1}^{g}e_if_i=\sum\limits_{i=1}^{g}ef=efg$. 并且 $\mathfrak{p}O_L=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$.

(d) 由于范 $N_{L/K}$ 是积性函数, 从而只需考虑 L 中的素理想 $\mathfrak{P}$ 即可. 设 $\mathfrak{P}\cap O_K=\mathfrak{p}$, $\mathfrak{p}O_K=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$, $\mathfrak{P}=\mathfrak{P}_1$, $n=efg$. 令 $D_{\mathfrak{P}}$ 为 G 中固定 $\mathfrak{P}$ 的子群, 即 $D_{\mathfrak{P}}=\{\sigma\in G|\sigma(\mathfrak{P})=\mathfrak{P}\}$. 由于 G 在集合 $\{\mathfrak{P}=\mathfrak{P}_1,\mathfrak{P}_2,\cdots,\mathfrak{P}_g\}$ 上是可迁的, 从而 $|D_{\mathfrak{P}}|=|G|/g=n/g=ef$. 并且有陪集分解

$$G=\sigma_1D_{\mathfrak{P}}\cup\sigma_2D_{\mathfrak{P}}\cup\cdots\cup\sigma_gD_{\mathfrak{P}},\ \sigma_i(\mathfrak{P})=\mathfrak{P}_i(1\leqslant i\leqslant g).$$

于是 $\prod\limits_{\sigma\in G}\sigma(\mathfrak{P})=\prod\limits_{i=1}^{g}\sigma_i(\prod\limits_{\sigma\in D_{\mathfrak{P}}}\sigma(\mathfrak{P}))=\prod\limits_{i=1}^{g}\sigma_i(\mathfrak{P}^{ef})=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^{ef}=(\mathfrak{p}O_L)^f=N_{L/K}(\mathfrak{P})O_L$. ∎

3.2 分解群和惯性群

我们在定理 12 的证明中曾经指出, 对于数域的伽罗华扩张 L/K 和域 L 的每个素理想 $\mathfrak{P}$, $D_{\mathfrak{P}}=\{\sigma\in\mathrm{Gal}(L/K)|\sigma(\mathfrak{P})=\mathfrak{P}\}$ 是 $\mathrm{Gal}(L/K)$ 的 ef 阶子群. 称作是 $\mathfrak{P}$(对于伽罗华扩张 L/K)的**分解群**. 令 $\overline{L}=O_L/\mathfrak{P}$, $\overline{K}=O_{K}/\mathfrak{p}$(其中 $\mathfrak{p}=\mathfrak{P}\cap O_K$), 则 $\overline{L}$ 和 $\overline{K}$ 均是有限域, 并且 $\overline{L}$ 是 $\overline{K}$ 的 f 次扩域. 对于每个 $\sigma\in D_{\mathfrak{P}}$, 由于 $\sigma(\mathfrak{P})=\mathfrak{P}$, 从而可以定义如下的映射:

$$\bar{\sigma}:\overline{L}\to\overline{L},\ \bar{\sigma}(\bar{a})=\overline{\sigma(a)}\quad(a\in O_L,\ \bar{a}=a+\mathfrak{P}).$$

这个映射有如下的性质:

(1) 首先,映射 $\bar{\sigma}$ 是可以定义的. 因为若 $a, b \in O_L$, $\bar{a}=\bar{b}$, 则 $a-b\in\mathfrak{P}$, 从而 $\sigma(a)-\sigma(b)=\sigma(a-b)\in\sigma(\mathfrak{P})=\mathfrak{P}$, 即 $\bar{\sigma}(\bar{a})=\overline{\sigma(a)}=\overline{\sigma(b)}=\bar{\sigma}(\bar{b})$, 即 $\bar{\sigma}(\bar{a})$ 与剩余类 $\bar{a}$ 中代表元 a 的选取无关.

(2) $\bar{\sigma}$ 是域 $\bar{L}$ 的自同构. 因为

$$\begin{aligned}\bar{\sigma}(\bar{a}\pm\bar{b})&=\overline{\sigma(a\pm b)}=\overline{\sigma(a)\pm\sigma(b)}=\overline{\sigma(a)}\pm\overline{\sigma(b)}\\&=\bar{\sigma}(\bar{a})\pm\bar{\sigma}(\bar{b}),\end{aligned}$$

类似地 $\bar{\sigma}(\bar{a}\cdot\bar{b})=\bar{\sigma}(\bar{a})\cdot\bar{\sigma}(\bar{b})$. 从而 $\bar{\sigma}$ 是域 $\bar{L}$ 的自同态. 进而

$$\begin{aligned}\operatorname{Ker}\bar{\sigma}&=\{\bar{a}\mid\overline{\sigma(a)}=\bar{0}\}=\{\bar{a}\mid\sigma(a)\in\mathfrak{P}\}\\&=\{\bar{a}\mid a\in\sigma^{-1}(\mathfrak{P})=\mathfrak{P}\}=\{\bar{0}\},\end{aligned}$$

从而 $\bar{\sigma}$ 是单同态. 最后,由于 $\bar{L}$ 是有限域, 从而 $\bar{\sigma}$ 也必然是满同态,即 $\bar{\sigma}$ 是域 $\bar{L}$ 的自同构.

(3) $\bar{\sigma}$ 固定 $\bar{K}$ 中每个元素. 这是因为: 若 $\bar{a}\in\bar{K}$, $a\in O_K$, 则 $\bar{\sigma}(\bar{a})=\overline{\sigma(a)}=\bar{a}$.

由以上即知, 对于每个 $\sigma\in D_{\mathfrak{P}}$, 我们按上述方式定义出的 $\bar{\sigma}$ 属于 $\bar{L}/\bar{K}$ 的伽罗华群 $\mathrm{Gal}(\bar{L}/\bar{K})$. 从而又给出映射:

$$\pi:\ D_{\mathfrak{P}}\to\mathrm{Gal}(\bar{L}/\bar{K}),\ \pi(\sigma)=\bar{\sigma}.$$

引理 16 π 是群的满同态, 并且 $\operatorname{Ker}\pi$ 为 $I_{\mathfrak{P}}=\{\sigma\in D_{\mathfrak{P}}\mid\sigma(\alpha)\equiv\alpha\pmod{\mathfrak{P}}$, 对每个 $\alpha\in O_L\}$. $|I_{\mathfrak{P}}|=e$, $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ 为 f 阶循环群.

证明 设 $\sigma, \tau\in D_{\mathfrak{P}}$, 则对每个 $\bar{\alpha}\in\bar{L}$, $\alpha\in O_L$, 均有

$$\overline{\sigma\tau}(\bar{\alpha})=\overline{\sigma\tau(\alpha)}=\bar{\sigma}\,\overline{(\tau(\alpha))}=\bar{\sigma}\bar{\tau}(\bar{\alpha}),$$

因此 $\overline{\sigma\tau}=\bar{\sigma}\bar{\tau}$, 这表明 π 是群的同态. 为证 π 是满同态, 只需证明对每个 $\tilde{\sigma}\in\mathrm{Gal}(\bar{L}/\bar{K})$, 均存在 $\sigma\in D_{\mathfrak{P}}$ 使得 $\bar{\sigma}=\tilde{\sigma}$. 我们知道, 有限域扩张 $\bar{L}/\bar{K}$ 均是单扩张 $\bar{L}=\bar{K}(\bar{\alpha})$, $\alpha\in O_L$(附录 B, IV). 以 K_D 表示 L 的子域, 它在伽罗华对应下对应于群 $D_{\mathfrak{P}}$, 即

$$K_D=\{\alpha\in L\mid\sigma(\alpha)=\alpha, \text{对于每个 }\sigma\in D_{\mathfrak{P}}\}.$$

从伽罗华扩张基本定理(附录 B, (16))知道 $L\supseteq K_D\supseteq K$, L/K_D 是 ef 次伽罗华扩张, 并且 $\mathrm{Gal}(L/K_D)=D_{\mathfrak{P}}$. 令 $O_D=O_{K_D}$, $\mathfrak{P}\cap$

$O_D=\mathfrak{P}_D$，则 $\mathfrak{P}_D\cap O_K=\mathfrak{P}\cap O_K=\mathfrak{p}$. 从而我们有下边的图表.

由于 $\mathrm{Gal}(L/K_D)=D_{\mathfrak{P}}$，而对 $\sigma\in D_{\mathfrak{P}}$ 均有 $\sigma(\mathfrak{P})=\mathfrak{P}$. 从定理 12(b) 即知 $\mathfrak{P}$ 对于扩张 L/K_D 是自共轭的. 因此 $\mathfrak{P}_D$ 在 L 中的素理想分解为 $\mathfrak{P}_DO_L=\mathfrak{P}^{e'}$. $e'=e(\mathfrak{P}/\mathfrak{P}_D)$. 令 $f'=f(\mathfrak{P}|\mathfrak{P}_D)$，则 $e'\cdot e(\mathfrak{P}_D|_{\mathfrak{p}})=e(\mathfrak{P}/\mathfrak{p})=e$, $f'\cdot f(\mathfrak{P}_D|\mathfrak{p})=f(\mathfrak{P}/\mathfrak{p})=f$. 但是 $e'f'=[L:K_D]=ef$，这就表明 $e'=e$, $f'=f$，并且 $e(\mathfrak{P}_D/\mathfrak{p})=f(\mathfrak{P}_D/\mathfrak{p})=1$. 特别地我们得到 $O_D/\mathfrak{P}_D=O_K/\mathfrak{p}$. 令 α 在 K_D 上的极小多项式为

$$\begin{array}{cccl} \mathfrak{P} & L & \{1\} & \\ | & | & | & \Big\} ef \\ \mathfrak{P}_D & K_D & D_{\mathfrak{P}} & \\ | & | & | & \Big\} g \\ \mathfrak{p} & K & \mathrm{Gal}(L/K) & \end{array}$$

$$f(x)=x^r+a_1x^{r-1}+\cdots+a_r,\ a_i\in O_D,$$

则 $f(x)$ 的每个根均有形式 $\sigma(\alpha)$, $\sigma\in\mathrm{Gal}(L/K_D)=D_{\mathfrak{P}}$. 将 $f(x)$ 的系数模 $\mathfrak{P}_D$ 之后，得到 $\bar{f}(x)=x^r+\bar{a}_1x^{r-1}+\cdots+\bar{a}_r\in O_D/\mathfrak{P}_D[x]$. 由于 $O_D/\mathfrak{P}_D=O_K/\mathfrak{p}=\overline{K}$，从而 $\bar{a}_i$ 中可取代表元(仍记为 a_i)属于 $O_K(1\leqslant i\leqslant r)$. 因此可认为 $\bar{f}(x)\in\overline{K}[x]$. 而这时 $\bar{f}(x)$ 的每个根均有形式 $\overline{\sigma(\alpha)}=\bar{\sigma}(\bar{\alpha})$. 由于 $\bar{\alpha}$ 在 $\overline{K}$ 上的极小多项式为 $\bar{f}(x)$ 的因式，从而 $\bar{\alpha}$ 的 $\overline{K}$-共轭元 $\tilde{\sigma}(\bar{\alpha})$ 是 $\bar{f}(x)$ 的根. 从而 $\tilde{\sigma}(\bar{\alpha})$ 必有形式 $\overline{\sigma(\alpha)}=\bar{\sigma}(\bar{\alpha})$. 这就表明存在 $\sigma\in D_{\mathfrak{P}}$，使得 $\bar{\sigma}(\bar{\alpha})=\tilde{\sigma}(\bar{\alpha})$. 由于 $\overline{L}=\overline{K}(\bar{\alpha})$，因此 $\bar{\sigma}=\tilde{\sigma}$. 即 $\pi: D_{\mathfrak{P}}\to\mathrm{Gal}(\overline{L}/\overline{K})$ 是满同态.

最后，

$$\begin{aligned}\mathrm{Ker}\,\pi&=\{\sigma\in D_{\mathfrak{P}}\,|\,\bar{\sigma}=1\}=\{\sigma\in D_{\mathfrak{P}}\,|\,\bar{\sigma}(\bar{\alpha})=\bar{\alpha},\text{对于每个 }\bar{\alpha}\in\overline{L}\}\\&=\{\sigma\in D_{\mathfrak{P}}\,|\,\sigma(\alpha)\equiv\alpha\,(\mathrm{mod}\,\mathfrak{P}),\text{对于每个 }\alpha\in O_L\}=I_{\mathfrak{P}}.\end{aligned}$$

从而 $D_{\mathfrak{P}}/I_{\mathfrak{P}}\cong\mathrm{Gal}(\overline{L}/\overline{K})$. 但是右边为 f 阶循环群（附录 B, (17)），从而 $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ 也是如此，这就完成了引理的证明. ∎

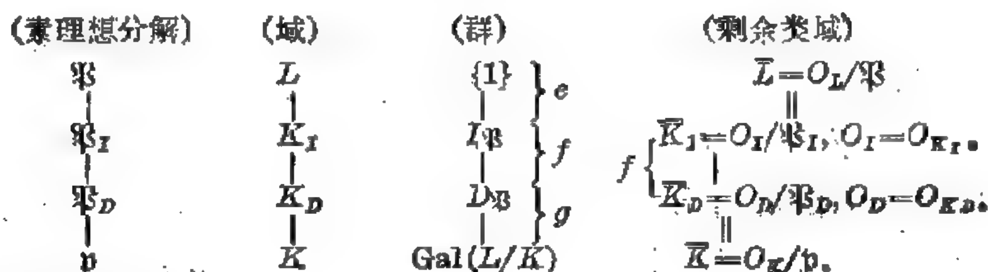
引理 16 中的群 $I_{\mathfrak{P}}$ 叫作是 $\mathfrak{P}$(对于伽罗华扩张 L/K) 的惯性群. 这是分解群 $D_{\mathfrak{P}}$ 的 e 阶正规子群，并且 $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ 为 f 阶循环群. 在伽罗华对应下，分解群 $D_{\mathfrak{P}}$ 对应的域 $K_D=\{\alpha\in L\,|\,\sigma(\alpha)=\alpha$, 对每个 $\sigma\in D_{\mathfrak{P}}\}$ 叫作是 $\mathfrak{P}$ 的分解域，而惯性群 $I_{\mathfrak{P}}$ 对应的域 $K_I=\{a\in L\,|\,\sigma(\alpha)=\alpha$, 对每个 $\sigma\in I_{\mathfrak{P}}\}$ 叫作是 $\mathfrak{P}$ 的惯性域. 于是我们有 $K\subseteq K_D\subseteq K_I\subseteq L$, $[L:K_I]=e$, $[K_I:K_D]=|D_{\mathfrak{P}}/I_{\mathfrak{P}}|=f$, $[K_D:K]=g$.

定理 13 设 L/K 为数域的伽罗华扩张，$n=[L:K]$. K 中

素理想 $\mathfrak{p}$ 在 L 中的素理想分解式为

$$\mathfrak{p}O_L=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e,\ f=f(\mathfrak{P}_i/\mathfrak{p})\ (1\leqslant i\leqslant g),$$
$$n=efd,\ \mathfrak{P}=\mathfrak{P}_1.$$

令 $D_{\mathfrak{P}}$, $I_{\mathfrak{P}}$, K_D, K_I 分别是 $\mathfrak{P}$ 对于伽罗华扩张 L/K 的分解群、惯性群、分解域和惯性域，则我们有如下的图表：



具体说来就是：

(a) L/K_I, L/K_D 和 K_I/K_D 均是伽罗华扩张，其伽罗华群分别为 $I_{\mathfrak{P}}$, $D_{\mathfrak{P}}$ 和 $D_{\mathfrak{P}}/I_{\mathfrak{P}}\cong\mathrm{Gal}(\overline{L}/\overline{K})$.

(b) 令 $\mathfrak{P}_I=\mathfrak{P}\cap O_I$, $\mathfrak{P}_D=\mathfrak{P}\cap O_D$, 则：

(i) $\mathfrak{p}=\mathfrak{P}_D\cap O_K$, $e(\mathfrak{P}_D/\mathfrak{p})=f(\mathfrak{P}_D/\mathfrak{p})=1$, 并且当 $D_{\mathfrak{P}}$ 为 $\mathrm{Gal}(L/K)$ 的正规子群时，$\mathfrak{p}$ 在 K_D 中完全分裂；

(ii) $\mathfrak{P}_DO_I=\mathfrak{P}_I$, $f(\mathfrak{P}_I/\mathfrak{P}_D)=f$（即 $\mathfrak{P}_D$ 在 K_I 中是惯性的，并且剩余类域次数为 f）；

(iii) $\mathfrak{P}_IO_L=\mathfrak{P}^e$, $f(\mathfrak{P}/\mathfrak{P}_I)=1$（即 $\mathfrak{P}_I$ 在 L 中完全分歧）.

(c) 对于每个 $\sigma\in\mathrm{Gal}(L/K)$, 则 $D_{\sigma(\mathfrak{P})}=\sigma D_{\mathfrak{P}}\sigma^{-1}$, $I_{\sigma(\mathfrak{P})}=\sigma I_{\mathfrak{P}}\sigma^{-1}$, $K_{I\sigma(\mathfrak{P})}=\sigma(K_{I\mathfrak{P}})$, $K_{D\sigma(\mathfrak{P})}=\sigma(K_{D\mathfrak{P}})$.

证明

(a) 由伽罗华理论即可证得（注意：K_I/K_D 为伽罗华扩张是由于 $I_{\mathfrak{P}}$ 为 $D_{\mathfrak{P}}$ 的正规子群）.

(b) 由于 $e=e(\mathfrak{P}/\mathfrak{p})=e(\mathfrak{P}/\mathfrak{P}_I)e(\mathfrak{P}_I/\mathfrak{P}_D)e(\mathfrak{P}_D/\mathfrak{p})$, $f=f(\mathfrak{P}/\mathfrak{p})=f(\mathfrak{P}/\mathfrak{P}_I)\cdot f(\mathfrak{P}_I/\mathfrak{P}_D)\cdot f(\mathfrak{P}_D/\mathfrak{p})$. 我们在引理 16 的证明中已经得出 $e(\mathfrak{P}_D/\mathfrak{p})=f(\mathfrak{P}_D/\mathfrak{p})=1$, 即 $e(\mathfrak{P}/\mathfrak{P}_D)=e(\mathfrak{P}/\mathfrak{P}_I)e(\mathfrak{P}_I/\mathfrak{P}_D)=e$, $f(\mathfrak{P}/\mathfrak{P}_D)=f(\mathfrak{P}/\mathfrak{P}_I)f(\mathfrak{P}_I/\mathfrak{P}_D)=f$. 并且当 $D_{\mathfrak{P}}$ 为 $\mathrm{Gal}(L/K)$ 的正规子群时，K_D/K 为伽罗华扩张，即知 $\mathfrak{p}$ 在 K_D 中完全分

裂. 继而考虑伽罗华扩张 L/K_I. 由定义不难看出 $\mathfrak{P}$ 对于扩张 L/K_I 的分解群和惯性群均是 $I_{\mathfrak{P}}$, 因此 $f(\mathfrak{P}/\mathfrak{P}_I)=|I_{\mathfrak{P}}/I_{\mathfrak{P}}|=1$. 于是 $f(\mathfrak{P}_I/\mathfrak{P}_D)=f$, $e(\mathfrak{P}/\mathfrak{P}_I)=[L:K_I]/f(\mathfrak{P}/\mathfrak{P}_I)=e/1=e$, $e(\mathfrak{P}_I/\mathfrak{P}_D)=f/f(\mathfrak{P}_I/\mathfrak{P}_D)=1$.

(c) 由于 $\tau\in D_{\mathfrak{P}}\Leftrightarrow\tau(\mathfrak{P})=\mathfrak{P}\Leftrightarrow\sigma\tau\sigma^{-1}(\sigma(\mathfrak{P}))=\sigma(\mathfrak{P})\Leftrightarrow\sigma\tau\sigma^{-1}\in D_{\sigma(\mathfrak{P})}$, 这就表明 $D_{\sigma(\mathfrak{P})}=\sigma D_{\mathfrak{P}}\sigma^{-1}$. 类似可证 $I_{\sigma(\mathfrak{P})}=\sigma I_{\mathfrak{P}}\sigma^{-1}$. 另一方面,

$$\begin{aligned}\alpha\in K_{D\mathfrak{P}}&\Leftrightarrow\tau(\alpha)=\alpha(\text{对每个 }\tau\in D_{\mathfrak{P}})\\&\Leftrightarrow\sigma\tau\sigma^{-1}(\sigma(\alpha))=\sigma(\alpha)(\text{对每个 }\sigma\tau\sigma^{-1}\in\\&\quad\sigma D_{\mathfrak{P}}\sigma^{-1}=D_{\sigma(\mathfrak{P})})\Leftrightarrow\sigma(\alpha)\in K_{D\sigma(\mathfrak{P})},\end{aligned}$$

从而 $K_{D\sigma(\mathfrak{P})}=\sigma(K_{D\mathfrak{P}})$. 同样可证 $K_{I\sigma(\mathfrak{P})}=\sigma(K_{I\mathfrak{P}})$. ∎

注记 设 L/K 为数域的伽罗华扩张. 如果其伽罗华群 $\mathrm{Gal}(L/K)$ 为 Abel 群,我们也称 L/K 为 **Abel 扩张**. 类似地,如果 $\mathrm{Gal}(L/K)$ 是循环群,也称 L/K 是循环扩张. 从定理 13 可以看出,对于 Abel 扩张 L/K, 若 K 的素理想 $\mathfrak{p}$ 在 L 中分解为 $\mathfrak{p}=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$, 则 $D_{\mathfrak{P}_i}(1\leqslant i\leqslant g)$ 均相等. 我们可以将它表示成 $D_{\mathfrak{p}}$, 叫作是 $\mathfrak{p}$(对于 L/K)的**分解群**. 类似地, $I_{\mathfrak{P}_i}(1\leqslant i\leqslant g)$ 也均相等, 表示成 $I_{\mathfrak{p}}$, 叫作是 $\mathfrak{p}$(对于 L/K)的**惯性群**. 在伽罗华对应下, $D_{\mathfrak{p}}$ 和 $I_{\mathfrak{p}}$ 对应的域分别为 K_D 和 K_I, 后者也分别称作是 $\mathfrak{p}$ 的**分解域**和**惯性域**. 于是当 L/K 为 Abel 扩张时, 可以把定理 13 粗略地叙述为: $\mathfrak{p}$ 在分解域 K_D 中完全分裂: $\mathfrak{p}O_D=\mathfrak{P}_{D,1}\cdots\mathfrak{P}_{D,g}$; 每个 $\mathfrak{P}_{D,i}$ 在惯性域 K_I 中均惯性: $\mathfrak{P}_{D,i}O_I=\mathfrak{P}_{I,i}(1\leqslant i\leqslant g)$, $f(\mathfrak{P}_{I,i}/\mathfrak{P}_{D,i})=f$; 最后, 每个 $\mathfrak{P}_{I,i}$ 在 L 中均完全分歧: $\mathfrak{P}_{I,i}O_L=\mathfrak{P}_i^e$, 总的结果为 $\mathfrak{p}O_L=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$.

3.3 Frobenius 自同构

设 L/K 为数域的伽罗华扩张. 如果 K 的素理想 $\mathfrak{p}$ 在 L 中不分歧, 即 $\mathfrak{p}O_L=\mathfrak{P}_1\cdots\mathfrak{P}_g$. $\mathfrak{P}=\mathfrak{P}_1$, 则由定理 13 可知 $I_{\mathfrak{P}}=\{1\}$, 而 $D_{\mathfrak{P}}$ 是 f 阶循环群, 并且 $D_{\mathfrak{P}}$ 正则同构于剩余类域的伽罗华群 $\mathrm{Gal}(\overline{L}/\overline{K})$. 注意 $|\overline{K}|=|O_K/\mathfrak{p}|=N_{K/\mathbf{Q}}(\mathfrak{p})$ (以下简记作 $N(\mathfrak{p})$).

从而 $\mathrm{Gal}(\bar{L}/\bar{K})$ 是由 f 阶元素 σ: $\gamma\mapsto\gamma^{N(\mathfrak{p})}(\gamma\in\bar{L})$ 所生成的(附录 B(17)). 在正则同构之下, $D_{\mathfrak{P}}$ 中对应于 σ 的元素表示成 $\left(\frac{L/K}{\mathfrak{P}}\right)$, 它是 f 阶元素并且生成 $D_{\mathfrak{P}}$. 我们将 $\left(\frac{L/K}{\mathfrak{P}}\right)$ 叫作是 $\mathfrak{P}$ 对于 L/K 的**Frobenius 自同构**. $D_{\mathfrak{P}}$ 中的 Frobenius 自同构这个元素可以用

$$\left(\frac{L/K}{\mathfrak{P}}\right)\alpha\equiv\alpha^{N(\mathfrak{p})}(\bmod\mathfrak{P})\quad(\text{对每个 }\alpha\in O_L)$$

来刻划. 这是因为: 如果 $\tau\in D_{\mathfrak{P}}$ 并且对每个 $\alpha\in O_L$ 均有 $\tau\alpha\equiv\alpha^{N(\mathfrak{p})}$ $(\bmod\mathfrak{P})$, 则在正则同构 $D_{\mathfrak{P}}\cong\mathrm{Gal}(\bar{L}/\bar{K})$, $\tau\mapsto\bar{\tau}$ 之下, 对每个 $\bar{\alpha}\in\bar{L}$ 均有 $\bar{\tau}(\bar{\alpha})=\bar{\alpha}^{N(\mathfrak{p})}$, 即 $\bar{\tau}=\sigma$, 从而 $\tau=\left(\frac{L/K}{\mathfrak{P}}\right)$.

关于 Frobenius 自同构的基本性质为:

引理 17 设 L/K 为数域的伽罗华扩张, $\mathfrak{P}|\mathfrak{p}$, 其中 $\mathfrak{P}$ 和 $\mathfrak{p}$ 分别为 L 和 K 的素理想, 并且 $e(\mathfrak{P}/\mathfrak{p})=1$, 则

(a) 对于每个 $\sigma\in\mathrm{Gal}(L/K)$, $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)=\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$;

(b) 如果 E 是 L/K 的中间域(从而 L/E 为伽罗华扩张), $\mathfrak{P}\cap O_E=\mathfrak{P}_E$, 则 $e(\mathfrak{P}|\mathfrak{P}_E)=1$, 并且 $\left(\frac{L/E}{\mathfrak{P}}\right)=\left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{P}_E/\mathfrak{p})}$.

(c) 如果 E/K 也是伽罗华扩张, 则 $e(\mathfrak{P}_E/\mathfrak{p})=1$, 并且 $\left(\frac{E/K}{\mathfrak{P}_E}\right)=\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_E\left(\left(\frac{L/K}{\mathfrak{P}}\right)\text{在 }E\text{ 上的限制}\right)$.

证明

(a) $\left(\frac{L/K}{\mathfrak{P}}\right)\alpha\equiv\alpha^{N(\mathfrak{p})}(\bmod\mathfrak{P})\ (\alpha\in O_L)\Rightarrow\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\sigma(\alpha))\equiv(\sigma(\alpha))^{N(\mathfrak{p})}(\bmod\sigma(\mathfrak{P}))(\alpha\in O_L)\Rightarrow\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}\alpha\equiv\alpha^{N(\mathfrak{p})}(\bmod\sigma(\mathfrak{P}))\ (\alpha\in O_L)\Rightarrow\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}=\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)$.

(b) $N_{E/\mathbb{Q}}(\mathfrak{P}_E)=N_{K/\mathbb{Q}}(\mathfrak{P})^{f(\mathfrak{P}_E/\mathfrak{p})}$

$$\Rightarrow\left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{P}_E/\mathfrak{p})}\alpha\equiv\alpha^{N_{K/\mathbb{Q}}(\mathfrak{p})^{f(\mathfrak{P}_E/\mathfrak{p})}}$$

$$=\alpha^{N_{E/\mathbb{Q}}(\mathfrak{P}_E)}(\bmod\mathfrak{P})\ (\alpha\in O_L)$$

$$\Rightarrow\left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{P}_E/\mathfrak{p})}=\left(\frac{L/E}{\mathfrak{P}}\right).$$

(c). 由于$\left(\frac{L/K}{\mathfrak{P}}\right)\alpha\equiv\alpha^{N(\mathfrak{p})}\pmod{\mathfrak{P}}$ $(\alpha\in O_L)$，而$\mathfrak{P}\cap O_E=\mathfrak{P}_E$，从而对$\alpha\in O_E$有$\left(\frac{L/K}{\mathfrak{P}}\right)\alpha\equiv\alpha^{N(\mathfrak{p})}\pmod{\mathfrak{P}_E}$，这就表明$\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_E=\left(\frac{E/K}{\mathfrak{P}_E}\right)$. ∎

作为引理 17 的应用，我们有如下的引理 18，在第五章中要用到它.

引理 18

(a) 设 E_1/K, E_2/K 均是数域的伽罗华扩张，$L=E_1E_2$(域的合成，见附录 B，(III))，则 L/K 也是伽罗华扩张，并且 $\mathrm{Gal}(L/K)$同构于直积 $\mathrm{Gal}(E_1/K)\times\mathrm{Gal}(E_2/K)$的一个子群.

(b) K 中素理想$\mathfrak{p}$在 L 中不分歧$\Leftrightarrow\mathfrak{p}$在 E_1 和 E_2 中均不分歧.

(c) $\mathfrak{p}$在 L 中完全分裂$\Leftrightarrow\mathfrak{p}$在 E_1 和 E_2 中均完全分裂.

证明

(a) E_i/K $(i=1, 2)$ 为伽罗华扩张$\Rightarrow E_i$是某个多项式 $f_i(x)\in K[x]$的分裂域$(i=1, 2)\Rightarrow L=E_1E_2$是多项式$f_1(x)f_2(x)\in K[x]$的分裂域$\Rightarrow L/K$ 是伽罗华扩张. 进而，作映射

φ: $\mathrm{Gal}(L/K)\to\mathrm{Gal}(E_1/K)\times\mathrm{Gal}(E_2/K)$, $\sigma\mapsto(\sigma|_{E_1}, \sigma|_{E_2})$，

易知φ为群的单同态. 从而 $\mathrm{Gal}(L/K)$ 同构于 $\mathrm{Gal}(E_1/K)\times\mathrm{Gal}(E_2/K)$的子群$\varphi(\mathrm{Gal}(L/K))$.

(b) 设$\mathfrak{P}|\mathfrak{p}$, $\mathfrak{P}$为 L 的素理想. 又令$\mathfrak{P}_i=\mathfrak{P}\cap O_{E_i}$ $(i=1, 2)$. 若$\sigma\in D_{\mathfrak{P}}$，则$\sigma(\mathfrak{P})=\mathfrak{P}$. 从而$\sigma(\mathfrak{P}_i)=\sigma(\mathfrak{P}\cap O_{E_i})=\sigma(\mathfrak{P})\cap\sigma(O_{E_i})=\mathfrak{P}\cap O_{E_i}=\mathfrak{P}_i$，因此$\sigma|E_i\in D_{\mathfrak{P}_i}$ $(i=1, 2)$，即$\varphi(D_{\mathfrak{P}})\subseteq D_{\mathfrak{P}_1}\times D_{\mathfrak{P}_2}$. 同样可证$\varphi(I_{\mathfrak{P}})\subseteq I_{\mathfrak{P}_1}\times I_{\mathfrak{P}_2}$. 从而$\mathfrak{p}$在$E_i$中不分歧$(i=1, 2)\Leftrightarrow I_{\mathfrak{P}_1}=I_{\mathfrak{P}_2}=\{1\}\Rightarrow I_{\mathfrak{P}}=\{1\}\Rightarrow\mathfrak{p}$在 L 中不分歧. 反之，由$\mathfrak{p}$在 L 中不分歧显然可推得$\mathfrak{p}$在 L 的子域 E_i $(i=1, 2)$中也不分歧(第 4 节习题 5).

(c) 从引理 17 知道，$\varphi\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)=\left(\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_{E_1},\left(\frac{L/K}{\mathfrak{P}}\right)\Big|_{E_2}\right)$ $=\left(\left(\frac{E_1/K}{\mathfrak{P}_1}\right),\ \left(\frac{E_2/K}{\mathfrak{P}_2}\right)\right)$. 从而 $\mathfrak{p}$ 在 L 中完全分裂 $\Leftrightarrow e(\mathfrak{P}/\mathfrak{p})$ $=f(\mathfrak{P}/\mathfrak{p})=1\Leftrightarrow\left(\frac{L/K}{\mathfrak{P}}\right)=1\Leftrightarrow\left(\frac{E_1/K}{\mathfrak{P}_1}\right)=1,\ \left(\frac{E_2/K}{\mathfrak{P}_2}\right)=1\Leftrightarrow\mathfrak{p}$ 在 E_1 和 E_2 中均完全分裂. ∎

3.4 素数在分圆域中的分解

作为 Frobenius 自同构的又一个应用，现在我们给出分圆域中素理想分解的一个完全刻划. 我们已经知道，对于分圆域 $K=\mathbb{Q}(\zeta_m)$，$\zeta_m=e^{2\pi i/m}$，$m\not\equiv 2\pmod 4$，则 $K/\mathbb{Q}$ 是 $\varphi(m)$ 次伽罗华扩张，并且其伽罗华群 $\mathrm{Gal}(K/\mathbb{Q})$ 正则同构于 $(\mathbb{Z}/m\mathbb{Z})^\times$: $\sigma_a\mapsto\bar{a}$，($(a,m)=1$)，其中 σ_a 是 $\mathrm{Gal}(K/\mathbb{Q})$ 中满足 $\sigma_a(\zeta_m)=\zeta_m^a$ 的元素，而 $\bar{a}$ 为模 m 剩余类，于是 $K/\mathbb{Q}$ 是 Abel 扩张. ζ_m 在 $\mathbb{Q}$ 上的极小多项式是分圆多项式 $\Phi_m(x)=\sum\limits_{\substack{r=1\\(r,m)=1}}^{m}(x-\zeta_m^r)$. 最后，由伽罗华理论易知 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{[m,n]})$，$\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{(m,n)})$.

定理 14 设 $K=\mathbb{Q}(\zeta_m)$，$m\not\equiv 2\pmod 4$，则

(a) 素数 p 在 K 中不分歧的充要条件是 $p\nmid m$. 并且在这个时候，$pO_K=\mathfrak{p}_1\cdots\mathfrak{p}_g$，其中 $g=\frac{\varphi(m)}{f}$，而 $f=f(\mathfrak{p}_i/p)$ 等于 $p\pmod m$ 的阶数(即 f 是满足 $p^f\equiv 1\pmod m$ 的最小正整数).

(b) 如果 $p\mid m$，令 $m=p^l\cdot m'$，$p\nmid m'$，则 $pO_K=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^e$，其中 $e=\varphi(p^l)$，$g=\frac{\varphi(m')}{f}$，$f=f(\mathfrak{p}_i/p)$ 为 $p\pmod{m'}$ 的阶数.

证明

(a) 第一推断是由 Dedekind 判别式定理和 $|d(K)|=m^{\varphi(m)}/\prod\limits_{p\mid m}p^{\varphi(m)/(p-1)}$(第一章定理 12)推出. 至于第二推断，我们只需求出 $f(\mathfrak{p}/p)$ ($\mathfrak{p}=\mathfrak{p}_1$)的值即可. 但是 $f(\mathfrak{p}/p)$ 是 Frobenius 自同构的阶，而$\left(\frac{K/\mathbb{Q}}{p}\right)$由$\left(\frac{K/\mathbb{Q}}{p}\right)\alpha\equiv\alpha^p\pmod{\mathfrak{p}}$ ($\alpha\in O_K=\mathbb{Z}[\zeta_m]$) 所刻划.

特别地有

$$\left(\frac{K/\mathbb{Q}}{p}\right)\zeta_m \equiv \zeta_m^p \pmod{\mathfrak{p}}. \tag{*}$$

注意$\left(\frac{K/\mathbb{Q}}{p}\right)$是 $\mathrm{Gal}(K/\mathbb{Q})$ 中的元素，从而$\left(\frac{K/\mathbb{Q}}{p}\right)\zeta_m=\zeta_m^l$，$(l, m)=1$，因此$\left(\frac{K/\mathbb{Q}}{p}\right)$的阶即是满足 $l^f\equiv 1 \pmod m$ 的最小正整数 f. 为此我们只需再证 $l\equiv p \pmod m$ 即可. 由(*)式我们现在有 $\zeta_m^l\equiv\zeta_m^p \pmod{\mathfrak{p}}$. 令 $P(x)=x^m-1=\prod\limits_{i=0}^{m-1}(x-\zeta_m^i)$. 由于 $p\nmid m$ 而 $O_K/\mathfrak{p}$ 是特征 p 的有限域，从而将 $P(x)$ 和 $p(x)=mx^{m-1}$ 看作是 $O_K/\mathfrak{p}[x]$ 中多项式时，$P'(x)\neq 0$，并且 $(P(x), P'(x))=1$. 这表明 x^m-1 在域 $O_K/\mathfrak{p}$ 上没有重根，换句话说，ζ_m 看作是 $O_K/\mathfrak{p}$ 中元素时阶也是 m. 于是由 $\zeta_m^l\equiv\zeta_m^p \pmod{\mathfrak{p}}$ 得出 $l\equiv p \pmod m$. 从而证明了 $f(\mathfrak{p}/p)$ (即$\left(\frac{K/\mathbb{Q}}{p}\right)$的阶)等于满足 $p^f\equiv 1 \pmod m$ 的最小正整数 f.

(b) 令 $K_0=\mathbb{Q}(\zeta_{p^r})$，$K'=\mathbb{Q}(\zeta_{m'})$，则有如下的图表

$$\begin{array}{ccc} & K=\mathbb{Q}(\zeta_m) & \\ K_0=\mathbb{Q}(\zeta_{p^r}) & & K'=\mathbb{Q}(\zeta_{m'}) \\ & \mathbb{Q} & \end{array}$$

我们在第 4.4 小节的例 2 中已经证明了素数 p 在 K_0 中完全分歧，即 $pO_{K_0}=\mathfrak{p}_0^{\varphi(p^r)}$. 从而若 $\mathfrak{p}$ 为 K 中的素理想，$\mathfrak{p}|\mathfrak{p}_0$，则 $e(\mathfrak{p}|p)\geqslant e(\mathfrak{p}_0/p)=\varphi(p^r)$. 另一方面，由(a)可知 p 在 K' 中的分解为 $pO_{K'}=\mathfrak{p}_1'\cdots\mathfrak{p}_g'$，其中 $gf=\varphi(m')$，而 f 为 p 模 m' 的阶数. 由于

$$\begin{aligned}\varphi(m)=[K:\mathbb{Q}]&\geqslant f(\mathfrak{p}|p)e(\mathfrak{p}|p)g\geqslant f\cdot\varphi(p^r)g\\&=\varphi(m')\varphi(p^r)=\varphi(m),\end{aligned}$$

以及 $f(\mathfrak{p}|p)\geqslant f$，$e(\mathfrak{p}|p)\geqslant\varphi(p^r)$，可知必然 $f(\mathfrak{p}/p)=f$，$e(\mathfrak{p}|p)=\varphi(p^r)$，从而证明了定理 14. ∎

习　题

1. 证明本节 5.1 中定义的理想范 $N_{L/K}(\mathfrak{a})$ 满足那里的性质(I)—(V).

2. 设 $K/\mathbb{Q}$ 为数域的 Abel 扩张，K_I 是素数 p 对于扩张 $K/\mathbb{Q}$ 的惯性域。求证 K_I 是 K 中使 p 不分歧的最大子域。换句话说，如果 M 是 $K/\mathbb{Q}$ 的中间域，则 p 在 M 中不分歧 $\Leftrightarrow M\subseteq K_I$。

3. 设 $K=\mathbb{Q}(\sqrt{5}, \sqrt{-1})$。求证

   (a) $K/\mathbb{Q}$ 是 4 次伽罗华扩张。求该扩张的伽罗华群；

   (b) 有理素数中只有 2 和 5 在 K 中分歧，并且分歧指数均是 2；

   (c) 求 2 和 5 对于扩张 $K/\mathbb{Q}$ 的分解群，分解域，惯性群和惯性域；

   (d) 求证 $\mathbb{Q}(\sqrt{-5})\subseteq K$，并且 $\mathbb{Q}(\sqrt{-5})$ 中每个素理想在 K 中均不分歧。

4. 仿照上题的方法，试证明 $\mathbb{Q}(\sqrt{10})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{5})$，并且 $\mathbb{Q}(\sqrt{10})$ 中每个素理想在域 $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ 中均不分歧。

5. 设 α 是多项式 x^3-x+1 的实根，β, $\bar{\beta}$ 是此多项式的一对共轭复根，$K=\mathbb{Q}[\alpha]$。求证：

   (a) $\beta+\bar{\beta}=-\alpha$, $\beta\bar{\beta}=-\alpha^{-1}$, $[(\beta-\alpha)(\bar{\beta}-\alpha)(\beta-\bar{\beta})]^2=-23$；

   (b) $K(\sqrt{-23})=\mathbb{Q}(\alpha, \beta, \bar{\beta})$，并且 $K(\sqrt{-23})/\mathbb{Q}$ 是 6 次伽罗华扩张。求该扩张的伽罗华群；

   (c) 决定 $K(\sqrt{-23})$ 的全部子域。其中哪些是 $\mathbb{Q}$ 的伽罗华扩域？

   (d) 求证有理素数中只有 23 在 $K(\sqrt{-23})$ 中分歧，并且分歧指数为 2；（提示：23 在 K 中的素理想分解式为 $23O_K=\mathfrak{p}_1\mathfrak{p}_2^2$）

   (e) 求证 $K(\sqrt{-23})/\mathbb{Q}(\sqrt{-23})$ 是 3 次循环扩张，并且 $\mathbb{Q}(\sqrt{-23})$ 中每个素理想在 $K(\sqrt{-23})$ 中均不分歧。

注记 类域论中的一个著名结果是说：每个数域 K 均有极大 Abel 不分歧扩张 H_K，称作是 K 的 Hilbert 类域。换句话说，H_K 满足如下的性质：(i) H_K/K 是数域的 Abel 扩张；(ii) K 中每个素理想在 H_K 中均不分歧，(iii) 如果 L 为 K 的另一个 Abel 扩域，并且 K 中每个素理想在 L 中均不分歧，则 $L\subseteq H_K$。类域论中还证明了：扩张 H_K/K 的伽罗华群同构于数域 K 的理想类群 C_K（关于理想类群 C_K 的定义见第三章）。我们在第三章中将要证明：域 $K=\mathbb{Q}(\sqrt{-5})$，$\mathbb{Q}(\sqrt{10})$ 和 $\mathbb{Q}(\sqrt{-23})$ 的理想类群分别是 2，2，3 阶循环群。于是从习题 3–5 可知 $L=\mathbb{Q}(\sqrt{5}, \sqrt{-1})$，$\mathbb{Q}(\sqrt{2}, \sqrt{5})$ 和 $\mathbb{Q}(\sqrt{-23},\alpha)$（$\alpha$ 是多项式 x^3-x+1 的实根）分别是它们的 Hilbert 类域。在一般情形下，求一个数域 K

的 Hilbert 类域是代数数论中一个相当困难的问题。

6. 令 $K=\mathbb{Q}(\zeta)$, $\zeta=\zeta_5=e^{2\pi i/5}$. 求证 $d(K)=5^4$, 并且求 $p=2, 3, 5, 19$ 在 K 中的素理想分解式.
7. 设 $K=\mathbb{Q}(\omega)$, $\omega=\zeta_{25}$.
   (a) 求证 K 有唯一的一个 5 次子域 M;
   (b) 求 $p=2, 3, 5$ 在 M 中的素理想分解式和它们的分解域与惯性域;
   (c) 求证: 素数 p 在 M 中完全分裂 $\Leftrightarrow p\equiv\pm1, \pm7 \pmod{25}$.

§4 Kronecker-Weber 定理

我们知道,分圆域 $\mathbb{Q}(\zeta_m)$ 均是 Abel 数域, 因此分圆域的每个子域也是 Abel 数域. Kronecker 和 Weber 证明了上述命题的逆也是对的, 即: 每个 Abel 数域均是某个分圆域的子域. 本节的主要目的是来证明这个很不平凡的结果. 我们首先证明每个二次域均是分圆域的子域, 然后讲述 Hilbert 分歧理论——分歧群和分歧域. 最后用这一理论来证明 Kronecker-Weber 定理. 并且谈一下 Abel 域中的互反律.

4.1 二次域是分圆域的子域

二次域 $K=\mathbb{Q}(\sqrt{d})$ 是除了 $\mathbb{Q}$ 本身之外最简单的 Abel 数域, 其伽罗华群 $\mathrm{Gal}(K/\mathbb{Q})$ 是 2 元群. 对于二次域 K, 我们可以用明显的方式证明 K 是分圆域 $\mathbb{Q}(\zeta_m)$ 的子域,其中 $m=|d(K)|$. 证明的工具是 Gauss 和.

设 p 为奇素数, 对于每个 $a\in\mathbb{Z}$, $p\nmid a$, 我们曾经定义过 Legendre 符号:

$$\left(\frac{a}{p}\right)=\begin{cases}1, \text{如果 } a \text{ 为模 } p \text{ 的二次剩余;}\\ -1, \text{如果 } a \text{ 为模 } p \text{ 的非二次剩余.}\end{cases}$$

事实上, $\left(\frac{a}{p}\right)$ 显然只依赖于 a 的模 p 同余类, 从而我们定义了映射:

$$\left(\frac{}{p}\right): (\mathbb{Z}/p\mathbb{Z})^\times\to\{\pm1\},\ \bar{a}\mapsto\left(\frac{a}{p}\right).$$

熟知$(\mathbb{Z}/p\mathbb{Z})^\times$为$p-1$阶乘法循环群，即$(\mathbb{Z}/p\mathbb{Z})^\times=\langle\bar{g}\rangle$，其中$g$是模$p$的一个原根. 于是当$a\equiv g^{2t}(\bmod p)\left(0\leqslant t\leqslant\frac{p-3}{2}\right)$时，$\left(\frac{a}{p}\right)=1$，而当$a\equiv g^{2t+1}(\bmod p)\left(0\leqslant t\leqslant\frac{p-3}{2}\right)$时，$\left(\frac{a}{p}\right)=-1$. 由此不难看出，映射$\left(\frac{\cdot}{p}\right)$: $(\mathbb{Z}/p\mathbb{Z})^\times\to\{\pm1\}$是乘法群的满同态，即$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

设$\zeta_p=e^{2\pi i/p}$，定义

$$G_p(r)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^{ra}\quad(0\leqslant r\leqslant p-1).$$

称作是对于 Legendre 符号$\left(\frac{\cdot}{p}\right)$的 Gauss 和. 显然$G_p(r)\in\mathbb{Q}(\zeta_p)$.

定理 15 设p为奇素数，则

(a) $G_p(0)=0$;

(b) $G_p(r)=\left(\frac{r}{p}\right)G_p(1)\ (1\leqslant r\leqslant p-1)$;

(c) $G_p(1)^2=\left(\frac{-1}{p}\right)p$.

证明

(a) 由于$\left(\frac{a}{p}\right)(1\leqslant a\leqslant p-1)$恰好有一半为1一半为$-1$，因此$G_p(0)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$.

(b) 令$rr'\equiv1(\bmod p)$，则$\left(\frac{r'}{p}\right)\left(\frac{r}{p}\right)=\left(\frac{rr'}{p}\right)=\left(\frac{1}{p}\right)=1$，从而$\left(\frac{r'}{p}\right)=\left(\frac{r}{p}\right)$. 于是

$$G_p(r)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^{ar}=\sum_{a=1}^{p-1}\left(\frac{ar'}{p}\right)\zeta_p^{arr'}=\sum_{a=1}^{p-1}\left(\frac{r'}{p}\right)\left(\frac{a}{p}\right)\zeta_p^{a}$$
$$=\left(\frac{r'}{p}\right)\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^{a}=\left(\frac{r}{p}\right)G_p(1).$$

(c) $$G_p(1)^2=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{a+b}=\sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a\cdot ac}{p}\right)\zeta_p^{a+ac}$$
$$=\sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\zeta_p^{a(1+c)}$$

$$=\left(\frac{-1}{p}\right)(p-1)+\sum_{c=1}^{p-2}\left(\frac{c}{p}\right)\sum_{a=1}^{p-1}\zeta_p^{a(1+c)}$$

$$=\left(\frac{-1}{p}\right)(p-1)-\sum_{c=1}^{p-2}\left(\frac{c}{p}\right)=\left(\frac{-1}{p}\right)p. \quad \blacksquare$$

定理 16(二次互反律) 设 p 和 q 是不同的奇素数. 则

(a) $p\nmid a$ 时, $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$;

(b) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & 若\ p\equiv 1 \pmod 4,\\ -1, & 若\ p\equiv 3 \pmod 4;\end{cases}$

(c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$;

(d) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & 若\ p\equiv \pm 1 \pmod 8,\\ -1, & 若\ p\equiv \pm 3 \pmod 8.\end{cases}$

证明

(a) 若 $a\equiv g^{2t} \pmod p$, 则

$$a^{\frac{p-1}{2}}\equiv (g^{2t})^{\frac{p-1}{2}}=(g^{p-1})^t\equiv 1=\left(\frac{a}{p}\right) \pmod p.$$

若 $a\equiv g^{2t+1} \pmod p$, 则

$$a^{\frac{p-1}{2}}\equiv (g^{p-1})^t\cdot g^{\frac{p-1}{2}}\equiv -1=\left(\frac{a}{p}\right) \pmod p.$$

因此当 $p\nmid a$ 时, 总有 $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

(b) 从(a)我们知道, $\left(\frac{-1}{p}\right)\equiv (-1)^{\frac{p-1}{2}} \pmod p$. 但是同余式两边均为 ± 1, 而 $p\geqslant 3$. 因此只能是 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

(c) 我们在 $\mathbb{F}_q$ 的代数闭包 Ω_q 中取一个 p 次本原单位根 w (即 w 是多项式 $x^{p-1}+x^{p-2}+\cdots+x+1\in\mathbb{F}_q[x]$ 在 Ω_q 中的一个根). 于是可以定义取值于 Ω_q 中的 Gauss 和:

$$\tau_p(r)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)w^{ar}\in\Omega_q \quad (0\leqslant r\leqslant p-1).$$

与在 $\mathbb{C}$ 中的情形一样, 可以得到: $\tau_p(r)=\left(\frac{r}{p}\right)\tau_p(1)$ $(1\leqslant r\leqslant p-1)$, $\tau_p^2(1)=\left(\frac{-1}{p}\right)p$. 但是现在 Ω_q 为特征 q 的域, 所以

$$\tau_p(1)^q = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)^q w^{aq} = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) w^{aq} = \tau_p(q) = \left(\frac{q}{p}\right)\tau_p(1).$$

于是在 Ω_q 中我们有

$$\left(\frac{q}{p}\right) = \tau_p(1)^{q-1} = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}$$
$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

注意这是 Ω_q 中的等式，即 $\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod q$. 但是同余式两边均为 ± 1，而 $q \geqslant 3$. 因此 $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$，即 $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

(d) 定义

$$\theta: (\mathbb{Z}/8\mathbb{Z})^{\times} \to \{\pm 1\},\ \theta(a) = (-1)^{\frac{a^2-1}{8}}.$$

直接验证 θ 是乘法群的满同态，即 $\theta(ab) = \theta(a)\theta(b)$. 在 $\mathbb{F}_p$ 的代数闭包 Ω_p 中取一个 8 次本原单位根 w，于是 $w^4 = -1$. 定义取值于 Ω_p 的 Gauss 和:

$$\tau_8(r) = \sum_{a=1,3,5,7}\theta(a)w^{ar} = w^r + w^{7r} - w^{3r} - w^{5r}\ \ (0 \leqslant r \leqslant 7).$$

利用 θ 为同态，可以与上面一样地证得在 Ω_p 中有

$$\tau_8(r) = \theta(r)\tau_8(1)\ (1 \leqslant r \leqslant 7),\ \tau_8(1)^p = \tau_8(p) = \theta(p)\tau_8(1).$$

但是 $\qquad \tau_8(1) = w + w^7 - w^3 - w^5 = 2(w - w^3),\ \tau_8(1)^2 = 8.$

从而在 Ω_p 中有

$$(-1)^{\frac{p^2-1}{8}} = \theta(p) = \tau_8(1)^{p-1} = 8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right),$$

即 $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$，从而 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. ∎

定理 17 设 $K = \mathbb{Q}(\sqrt{d})$（$d \in \mathbb{Z}$ 无平方因子），$L = \mathbb{Q}(\zeta_{|d(K)|})$，则 $K \subseteq L$，并且 L 是包含 K 的最小分圆域.

证明 先证 K 是分圆域 L 的子域.

如果 $d = \pm p_1 \cdots p_s$，其中 $p_1, \cdots, p_s$ 是不同的奇素数. 记

$$p_i^* = \left(\frac{-1}{p_i}\right)p_i = (-1)^{\frac{p_i-1}{2}}p_i\ (1 \leqslant i \leqslant s),$$

则 $d=\pm p_1^*\cdots p_s^*$. 由于 $p_i^*\equiv 1\pmod 4$ $(1\leqslant i\leqslant s)$, 可知当 $d=p_1^*\cdots p_s^*$ 时, $d(K)=d$; 而当 $d=-p_1^*\cdots p_s^*$ 时, $d(K)=4d$. 对于 $d=p_1^*\cdots p_s^*$, 由于 Gauss 和 $G_{p_i}(1)\in\mathbb{Q}(\zeta_{p_i})$ 并且 $G_{p_i}(1)=\pm\sqrt{p_i^*}$ (定理 15, (c)), 从而 $\sqrt{p_i^*}\in\mathbb{Q}(\zeta_{p_i})$ $(1\leqslant i\leqslant s)$, 于是

$$\begin{aligned}\mathbb{Q}(\sqrt{d})&=\mathbb{Q}(\sqrt{p_1^*\cdots p_s^*})\subseteq\mathbb{Q}(\sqrt{p_1^*},\ \cdots,\ \sqrt{p_s^*})\\&\subseteq\mathbb{Q}(\zeta_{p_1},\ \cdots,\ \zeta_{p_s})=\mathbb{Q}(\zeta_{p_1\cdots p_s})=L.\end{aligned}$$

类似地, 如果 $d=-p_1^*\cdots p_s^*$, 则

$$\begin{aligned}\mathbb{Q}(\sqrt{d})&\subseteq\mathbb{Q}(\sqrt{-1},\ \sqrt{p_1^*},\ \cdots,\ \sqrt{p_s^*})\subseteq\mathbb{Q}(\zeta_4,\ \zeta_{p_1},\ \cdots,\ \zeta_{p_s})\\&=\mathbb{Q}(\zeta_{4p_1\cdots p_s})=L.\end{aligned}$$

如果 $d=\pm 2p_1^*\cdots p_s^*$, 则 $|d(K)|=8p_1\cdots p_s$, 而

$$\begin{aligned}\mathbb{Q}(\sqrt{d})&\subseteq\mathbb{Q}(\sqrt{\pm 2},\ \sqrt{p_1^*},\ \cdots,\ \sqrt{p_s^*})\subseteq\mathbb{Q}(\zeta_8,\ \zeta_{p_1},\ \cdots,\ \zeta_{p_s})\\&=\mathbb{Q}(\zeta_{8p_1\cdots p_s})=L.\end{aligned}$$

这就证明了: 在任何情形下均有 $K=\mathbb{Q}(\sqrt{d})\subseteq\mathbb{Q}(\zeta_{|d(K)|})=L$.

再证 L 的极小性, 即如果 $\mathbb{Q}(\sqrt{d})\subseteq\mathbb{Q}(\zeta_m)$, 要证 $|d(K)|\,|\,m$.

如果 $d=p_1^*\cdots p_s^*$, 则 p_i 在 $\mathbb{Q}(\sqrt{d})$ 中分歧. 从而也在 $\mathbb{Q}(\zeta_m)$ 中分歧. 由判别式定理即知 $p_i|m$. 于是 $|d(K)|=p_1\cdots p_s|m$. 如果 $d=-p_1^*\cdots p_s^*$, 则 $|d(K)|=4p_1\cdots p_s$. 于是除了 $p_i(1\leqslant i\leqslant s)$ 之外, 2 也在 $\mathbb{Q}(\sqrt{d})$ 中分歧. 从而 $2|m$. 但是 2 在 $\mathbb{Q}(\zeta_{2p_1\cdots p_s})=\mathbb{Q}(\zeta_{p_1\cdots p_s})$ 中不分歧, 从而 $4|m$. 因此 $|d(K)|=4p_1\cdots p_s|m$. 最后, 若 $d=\pm 2p_1^*\cdots p_s^*$, 与上面一样可证 $p_1\cdots p_s|m$. 从而 $\mathbb{Q}(\sqrt{\pm 2})\subseteq\mathbb{Q}(\sqrt{d},\ \sqrt{p_1^*},\ \cdots,\ \sqrt{p_s^*})\subseteq\mathbb{Q}(\zeta_m,\ \zeta_{p_1},\ \cdots,\ \zeta_{p_s})=\mathbb{Q}(\zeta_m)$. 易知包含 $\mathbb{Q}(\sqrt{\pm 2})$ 的最小分圆域为 $\mathbb{Q}(\zeta_8)$, 从而 $8|m$. 于是 $|d(K)|=8p_1\cdots p_s|m$. ∎

4.2 分歧群和分歧域

现在讲述数域扩张的 Hilbert 分歧理论. 设 $K/\mathbb{Q}$ 是数域的伽罗华扩张. $n=[K:\mathbb{Q}]$. $\mathfrak{p}$ 为 K 的素理想, $\mathfrak{p}|p$. 对于 $m\geqslant 0$, 定义

$$V_m=\{\sigma\in D_{\mathfrak{p}}\,|\,\sigma(\alpha)\equiv\alpha\pmod{\mathfrak{p}^{m+1}},\text{对于每个 }\alpha\in O_K\}.$$

这显然是分解群 $D_{\mathfrak{p}}$ 的子群, 并且 V_0 显然是惯性群 $I_{\mathfrak{p}}$. 于是我们

有子群序列

$$D_{\mathfrak{p}}\supseteq I_{\mathfrak{p}}=V_0\supseteq V_1\supseteq V_2\supseteq\cdots\supseteq V_m\supseteq\cdots.$$

定理 18 (a) $V_m(m\geqslant 0)$ 均是 $D_{\mathfrak{p}}$ 的正规子群;

(b) 存在 m, 使得 $V_m=\{1\}$;

(c) 令 $e(\mathfrak{p}/p)=e=e_0p^v$, $p\nmid e_0$, $v\geqslant 0$, 则 $I_{\mathfrak{p}}/V_1$ 是e_0 阶循环群, 并且 $e_0\mid N(\mathfrak{p})-1$. 特别当 $p\nmid e$ 时 $V_1=\{1\}$;

(d) 当 $m\geqslant 1$ 时, V_m/V_{m+1} 是初级 p-群 $(p,\cdots,p)$, 并且 $|V_m/V_{m+1}|=p^{v_m}\mid N(\mathfrak{p})$, 而 $|V_1|=p^v$.

证明 (a) 设 $\tau\in D_{\mathfrak{p}}$, $\sigma\in V_m(m\geqslant 0)$, 则 $\tau(\mathfrak{p})=\mathfrak{p}$. 因此 $\tau(\mathfrak{p}^{m+1})=\mathfrak{p}^{m+1}$. 对于每个 $\alpha\in O_K$, $\sigma(\alpha)-\alpha\in\mathfrak{p}^{m+1}$. 于是

$$\tau\sigma\tau^{-1}(\alpha)-\alpha=\tau(\sigma\tau^{-1}(\alpha)-\tau^{-1}(\alpha))\in\tau(\mathfrak{p}^{m+1})=\mathfrak{p}^{m+1}.$$

于是 $\tau\sigma\tau^{-1}\in V_m$, 即 V_m 为 $D_{\mathfrak{p}}$ 的正规子群.

(b) 设 $K=\mathbb{Q}(w)$, 则 $\sigma\in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma\neq 1$ 时, $\sigma(w)\neq w$, 从而有充分大的 m, 使得对每个 $\sigma\neq 1$ 均有 $\sigma(w)-w\notin\mathfrak{p}^{m+1}$. 于是 $V_m=\{1\}$.

(c) 取 $\pi\in\mathfrak{p}-\mathfrak{p}^2$. 由于 $O_I/\mathfrak{p}_I=O_K/\mathfrak{p}$, 可知对于每个 $\gamma\in O_K$ 均有 $\gamma_0\in O_I$ 使得 $\gamma\equiv\gamma_0 \pmod{\mathfrak{p}}$. 如此下去, 可知 O_K 中元素均可写成

$$\mu\equiv\gamma_0+\gamma_1\pi+\cdots+\gamma_m\pi^m \pmod{\mathfrak{p}^{m+1}},\ \gamma_i\in O_I.$$

于是对每个 $\sigma\in I_{\mathfrak{p}}$,

$$\sigma(\mu)-\mu\equiv\gamma_1(\sigma(\pi)-\pi)+\cdots+\gamma_m(\sigma(\pi)^m-\pi^m) \pmod{\mathfrak{p}^{m+1}}.$$

从而 $\sigma(\pi)-\pi\in\mathfrak{p}^{m+1}\Leftrightarrow\sigma(\mu)-\mu\in\mathfrak{p}^{m+1}$(对每个 $\mu\in O_K$) $\Leftrightarrow\sigma\in V_m$. 因此, 若令 $\nu(\sigma)=\nu_{\mathfrak{p}}(\sigma(\pi)-\pi)$ (符号 $\nu_{\mathfrak{p}}$ 的定义见 §3, 习题 13), 则 $\nu(\sigma)\geqslant m+1\Leftrightarrow\sigma\in V_m$. 现在对于每个 $\sigma\in I_{\mathfrak{p}}$, 由于 $\sigma(\mathfrak{p})=\mathfrak{p}$, 从而 $\sigma(\pi)\in\mathfrak{p}$, 而 $(\pi,\ \sigma(\pi),\ \mathfrak{p}^2)=\mathfrak{p}$, 于是同余方程 $\pi x\equiv\sigma(\pi) \pmod{\mathfrak{p}^2}$ 对于模 $\mathfrak{p}^2/(\pi,\ \mathfrak{p}^2)=\mathfrak{p}$ 有唯一解 $x\equiv\alpha_\sigma \pmod{\mathfrak{p}}$, $\alpha_\sigma\in O_K$ (§3, 习题 15), 从而也有模 $\mathfrak{p}_I$ 的唯一解 $\gamma_\sigma\in O_I$ 使得 $\sigma(\pi)=\pi\gamma_\sigma \pmod{\mathfrak{p}^2}$. 由于 $\sigma(\pi)\not\equiv 0 \pmod{\mathfrak{p}^2}$ 可知 $\gamma_\sigma\not\equiv 0 \pmod{\mathfrak{p}_I}$. 这样我们就定义了映射

$$\chi: I_{\mathfrak{p}} \to (O_I/\mathfrak{p}_I)^{\times}, \ \sigma \mapsto \gamma_\sigma (\bmod \mathfrak{p}_I).$$

χ 是群同态: 因为对于

$$\sigma_1, \ \sigma_2 \in I_{\mathfrak{p}}, \ \pi\gamma_{\sigma_1\sigma_2} \equiv \sigma_1\sigma_2(\pi) \equiv \sigma_1(\pi\gamma_{\sigma_2}) = \sigma_1(\pi)\gamma_{\sigma_2}$$
$$\equiv \pi\gamma_{\sigma_2}\gamma_{\sigma_1} (\bmod \mathfrak{p}^2),$$

即 $\gamma_{\sigma_1\sigma_2} \equiv \gamma_{\sigma_1}\gamma_{\sigma_2} (\bmod \mathfrak{p}_I)$. 进而,

$$\operatorname{Ker} \chi = \{\sigma \in I_{\mathfrak{p}} \mid \gamma_\sigma \equiv 1 (\bmod \mathfrak{p})\} = \{\sigma \in I_{\mathfrak{p}} \mid \sigma(\pi)$$
$$\equiv \pi (\bmod \mathfrak{p}^2)\} = V_1.$$

从而 $I_{\mathfrak{p}}/V_1$ 同构于 $(O_I/\mathfrak{p}_I)^{\times}$ 的一个子群. 但是 $(O_I/\mathfrak{p}_I)^{\times} \cong (O_K/\mathfrak{p})^{\times}$ 是 $N(\mathfrak{p})-1$ 阶循环群, 从而 $I_{\mathfrak{p}}/V_1$ 为 e' 阶循环群, 并且 $e' \mid N(\mathfrak{p})-1$. 下面我们证明 $|V_1| = p^v$. 由此推出 $e' = |I_{\mathfrak{p}}/V_1| = e_0 p^v / p^v = e_0$.

(d) 当 $m \geq 1$ 时, 与(c)中类似地可证得: 对于每个 $\sigma \in V_m$, 均存在模 $\mathfrak{p}_I$ 的唯一元素 $\delta_\sigma \in O_I$, 使得

$$\sigma(\pi) - \pi \equiv \pi^{m+1}\delta_\sigma (\bmod \mathfrak{p}^{m+2}).$$

作映射

$$\lambda: \ V_m \to O_I/\mathfrak{p}_I, \quad \sigma \mapsto \delta_\sigma (\bmod \mathfrak{p}_I),$$

则 λ 是 V_m 到加法群 $O_I/\mathfrak{p}_I$ 的同态: 这是因为当 $\sigma_1, \ \sigma_2 \in V_m$ 时,

$$\pi + \pi^{m+1}\delta_{\sigma_1\sigma_2} \equiv \sigma_1\sigma_2(\pi) \equiv \sigma_1(\pi + \pi^{m+1}\delta_{\sigma_2})$$
$$= \sigma_1(\pi) + \sigma_1(\pi)^{m+1}\delta_{\sigma_2}$$
$$\equiv \pi + \pi^{m+1}\delta_{\sigma_1} + \pi^{m+1}\delta_{\sigma_2} (\bmod \mathfrak{p}^{m+2}),$$

从而 $\delta_{\sigma_1\sigma_2} \equiv \delta_{\sigma_1} + \delta_{\sigma_2} (\bmod \mathfrak{p}_I)$. 这就表明 λ 是同态. 进而,

$$\operatorname{Ker} \lambda = \{\sigma \in V_m \mid \delta_\sigma \equiv 0 (\bmod \mathfrak{p})\} = \{\sigma \in V_m \mid \sigma(\pi)$$
$$\equiv \pi (\bmod \mathfrak{p}^{m+2})\} = V_{m+1},$$

从而 V_m/V_{m+1} 同构于 $O_I/\mathfrak{p}_I$ 的一个加法子群. 但是 $O_I/\mathfrak{p}_I$ 是特征 p 的域, $O_I/\mathfrak{p}_I$ 的加法群为初级 p 群. 因此 V_m/V_{m+1} 也是初级 p 群.

令 $|V_m/V_{m+1}| = p^{v_m}$. 由(b)知有 M, 使得 $|V_M| = 1$. 于是

$$|V_1| = |V_1/V_2| \cdot |V_2/V_3| \cdots |V_{M-1}/V_M| = p^t,$$
$$t = V_1 + V_2 + \cdots + V_{M-1}.$$

从而 $e = e_0 p^v = |I_{\mathfrak{p}}| = |I_{\mathfrak{p}}/V_1| \cdot |V_1| = e'p^t$. 由于 $e' \mid N(\mathfrak{p}) - 1 =$

$p^{f(\mathfrak{p}|p)}-1$，可知 $p\nmid e'$。又由于 $p\nmid e_0$，这就表明 $|V_1|=p^v$ 而 $|I_0/V_1|=e_0$。 ∎

4.3 Kronecker-Weber 定理

定理 19 每个 Abel 数域 K 均是某个分圆域的子域.

这个定理的证明要经过几次简化.

(一) 如果 $\mathbb{Q}$ 的每个 p^r 次循环扩域 K 均是分圆域的子域，则定理 19 成立.

证明 设 $K/\mathbb{Q}$ 是 Abel 扩张，$n=[K:\mathbb{Q}]$，则伽罗华群 $G=\mathrm{Gal}(K/\mathbb{Q})$ 为 n 阶 Abel 群. 但是有限 Abel 群是一些循环群的直积：$G=G_1\times\cdots\times G_l$，并且 G_i 均是素数幂阶，即 $|G_i|=p_i^{a_i}$ $(1\leqslant i\leqslant l)$. 以 K_i 表示 $\widetilde{G}_i=G_1\times\cdots\times G_{i-1}\times\{1\}\times G_{i+1}\times\cdots\times G_l$ 的固定子域，则由伽罗华理论可知 $\mathrm{Gal}(K_i/\mathbb{Q})\cong G_i$，即 K_i 是 $p_i^{a_i}$ 次循环域 $(1\leqslant i\leqslant l)$. 而 $K_1K_2\cdots K_l$ 在伽罗华对应下对应于子群 $\bigcap\limits_{i=1}^{l}\widetilde{G}_i=\{1\}$，从而 $K=K_1K_2\cdots K_l$. 如果假设每个 $p_i^{a_i}$ 次循环域 K_i 均是某个分圆域 $\mathbb{Q}(\zeta_{m_i})$ 的子域 $(1\leqslant i\leqslant l)$，则 $K=K_1\cdots K_l\subseteq\mathbb{Q}(\zeta_{m_1},\cdots,\zeta_{m_l})=\mathbb{Q}(\zeta_{[m_1,\cdots,m_l]})$. 从而每个 Abel 数域 K 均是分圆域的子域. ∎

因此，我们以下假设 K 是 p^m 次循环域. 记 $S(K)=\{$素数 $q\mid q\neq p,\ q$ 在 K 中分歧$\}$，这是一个有限集合，令 $s(K)=|S(K)|$.

(二) 设 q 为素数，$q\neq p$. 如果每个 $s(K')<n$ 且次数为 p 的幂的循环域 K' 均是分圆域的子域，那末每个 $s(K)=n$ 且次数为 p 的幂的循环域 K 也均是分圆域的子域.

证明 设 $s(K)=n$，K 是 p^m 次循环域，$q\in S(K)$. $\mathfrak{q}$ 为 K 中素理想，$\mathfrak{q}|q$，则 $q\nmid|G|=|\mathrm{Gal}(K/\mathbb{Q})|=p^m$. 从而对于 $\mathfrak{q}$ 的分歧群 $V_1=\{1\}$（定理 18(c)），而 $|I_q|=p^u$（由于 K 是 Abel 域，我们可以把 $I_{\mathfrak{q}}$ 写成 I_q）. 根据定理 18(c)知循环群 I_q 的阶 $p^u|N(\mathfrak{q})-1=q^{f(\mathfrak{q}|q)}-1$. 事实上，对于目前 D_q 为 Abel 群的情形，我们来

证明 $p^u|(q-1)$，考虑定理 18 证明中给出的同构：

$$\chi: I_q/V_1 = I_q \xrightarrow{\sim} (O_K/\mathfrak{q})^\times,\ \tau \mapsto \bar{a}_\tau (\bmod\ \mathfrak{q}),$$

$$\tau(\pi) = a_\tau \pi (\bmod\ \mathfrak{q}^2),\ a_\tau \in O_I - \mathfrak{q},\ \pi \in \mathfrak{q} - \mathfrak{q}^2.$$

令 $I_q = \langle\tau\rangle$，$\sigma = \left(\dfrac{K/\mathbb{Q}}{q}\right) \in D_q$ 为 $G(\overline{K}/\mathbb{Q})$ 的生成元 $\bar{\sigma}$ 的任一原象。为简化起见，记

$$\sigma\pi \equiv a\pi,\ \tau\pi \equiv b\pi (\bmod\ \mathfrak{q}^2),\quad a,\ b,\ \in O_K - \mathfrak{q}.$$

于是 $\sigma^{-1}\pi = (\sigma^{-1}(a))^{-1}\pi$。由 D_q 为 Abel 群可知

$$\begin{aligned} b\pi &\equiv \tau\pi \equiv \sigma\tau\sigma^{-1}(\pi) \equiv \sigma\tau[(\sigma^{-1}(a))^{-1}\pi] \\ &\equiv (\sigma\tau\sigma^{-1}(a))^{-1} \cdot \sigma\tau(\pi) \equiv \tau(a)^{-1} \cdot \sigma(b\pi) \\ &\equiv \tau(a)^{-1}\sigma(b)a\pi (\bmod\ \mathfrak{q}^2), \end{aligned}$$

这表明在上述同构下 τ 对应于 $\tau(a)^{-1}\sigma(b)a\pi$，从而

$$b = \tau(a)^{-1}\sigma(b)a.$$

由于对每个 $\gamma \in O_K$ 我们有 $\tau(\gamma) \equiv \gamma$，$\sigma(\gamma) \equiv \gamma^q (\bmod\ \mathfrak{q})$。因此 $b \equiv a^{-1}b^q a \equiv b^q (\bmod\ \mathfrak{q})$，从而 $b^{q-1} \equiv 1 (\bmod\ \mathfrak{q})$。由于在上述同构下 τ 与 b 对应，于是 $\tau^{q-1} = 1$。这就表明 τ 的阶除尽 $q-1$，即 $p^u|(q-1)$。

于是，$\mathbb{Q}(\zeta_q)$ 有唯一的 p^u 次循环子域 L。由于 q 在 $\mathbb{Q}(\zeta_q)$ 中完全分歧，从而 q 在 L 中也完全分歧，并且其他素数在 L 中均不分歧。现在考虑伽罗华扩张 $KL/\mathbb{Q}$。$[KL:\mathbb{Q}] = p^{m+v}$，$v \leqslant u$。设 $\mathfrak{q}'$ 为 KL 中的素理想，$\mathfrak{q}'|\mathfrak{q}$。$I'_q$ 为 $\mathfrak{q}'$ 对于 q 的惯性群，$H = \mathrm{Gal}(L/\mathbb{Q})$，$G = \mathrm{Gal}(K/\mathbb{Q})$。通过单同态

$$\varphi:\ \mathrm{Gal}(KL/\mathbb{Q}) \to G \times H (\text{直积}),\ \varphi(\sigma) = (\sigma|_K,\ \sigma|_L),$$

可以将 $\mathrm{Gal}(KL/\mathbb{Q})$ 看作是 $G \times H$ 的子群，并且 $\varphi(I'_q) \subseteq I_q \times H$。$|I'_q| = e(\mathfrak{q}'/q) \geqslant e(\mathfrak{q}/q) = |I_q| = p^u$。与对 $\mathfrak{q}$ 的情形一样，可以证出，对于 $\mathfrak{q}'$ 的分歧群 $V'_1 = \{1\}$。从而 I'_q 为循环群。但是 $I_q \times H$ 中没有阶数大于 p^u 的元素，因此 $|I'_q| = p^u$。设 K'_I 为对 $\mathfrak{q}'$ 的惯性域（即 I'_q 的固定子域），$\mathfrak{q}'_I = \mathfrak{q}' \cap O_{K'_I}$，则 $e(\mathfrak{q}'_I|q) = 1$。由于 q 在 L 中完全分歧，从而 $K'_I \cap L = \mathbb{Q}$，于是 $[K'_I L:\mathbb{Q}] = [K'_I:\mathbb{Q}][L:\mathbb{Q}]$。

但是 $[KL:K_I']=|I_q'|=p^n=[L:\mathbb{Q}]$，从而$[K_I'L:\mathbb{Q}]=[K_I':\mathbb{Q}]$，$[KL:K_I']=[KL:\mathbb{Q}]$，再由 $K_I'L\subseteq KL$ 可知 $K_I'L=KL$。注意 $s(K_I')<n$（这是由于 q 在K_I' 中不分歧．并且若素数 $q'(q'\neq q$, $q'\neq p)$在 K 中不分歧，则因为 q' 在 L 中也不分歧，从而 q' 在 KL 中也不分歧，于是 q' 在子域 K_I' 中也不分歧，因此 $s(K_I')<s(K)=n$）．由命题假设，K_I' 为分圆域的子域，于是 $K\subseteq KL=K_I'L\subseteq K_I'(\zeta_q)$ 也是分圆域的子域． ▌

基于（二），我们又将问题化为 K 是 p^v 次循环域并且 $s(K)=0$（即 p 以外的素数均不分歧）的情形．如果 p 在 K 中也不分歧，则 K 就是 $\mathbb{Q}$ 的不分歧扩张，我们在下一章要证明这时必然 $K=\mathbb{Q}$．从而以下只考虑 K 是 p^v 次循环域并且只有 p 在 K 中分歧的情形．我们先来说明确实有两种分圆域的子域具有这种性质：

(A)　$p\geqslant 3$，$L_1=\mathbb{Q}(\zeta_{p^{v+1}})\ (v\geqslant 1)$ 为 $\varphi(p^{v+1})=p^v(p-1)$ 次循环域，则 L_1 有唯一的 p^v 次循环子域 F_{p^v}，F_{p^v} 的每个子域 $\widetilde{K}$ 均是 p 幂次循环域，只有 p 在 $\widetilde{K}$ 中分歧，而且是完全分歧．

(B)　$p=2$，$L_2=\mathbb{Q}(\zeta_{2^{v+2}})\ (v\geqslant 1)$．$\mathrm{Gal}(L_2/\mathbb{Q})\cong(\mathbb{Z}/2^{v+2}\mathbb{Z})^\times=\langle -\bar{1}\rangle\times\langle\bar{5}\rangle$，其中 $\langle -\bar{1}\rangle$ 和 $\langle\bar{5}\rangle$ 分别是 2 阶和 2^v 阶循环群，$\sigma_{-1}(\zeta_{2^{v+2}})=\bar{\zeta}_{2^{v+2}}$，于是 $F_{2^{v+1}}=\mathbb{Q}(\zeta_{2^{v+2}}+\bar{\zeta}_{2^{v+2}})$ 为 2^v 次循环域，它的每个子域 $\widetilde{K}$ 均是 2 幂次循环域，只有 2 在 $\widetilde{K}$ 中分歧，并且是完全分歧．

现在我们来证明：

(三)　若 K 为 p 幂次循环域，并且只有 p 在 K 中分歧，则 K 必为 L_1 或 L_2 的上述某个子域 $\widetilde{K}$（视 $p\geqslant 3$ 和 $p=2$ 而定）．

为证此，我们需要下列两个引理．

引理 19　设 K 是 p 次循环域，p 为奇素数，并且只有 p 在 K 中分歧：$pO_K=\mathfrak{p}^p$．则 $G=I_\mathfrak{p}=V_1$，而 $V_2=\{1\}$（其中 $G=\mathrm{Gal}(K/\mathbb{Q})$，而 V_1 和 V_2 是对于 $\mathfrak{p}$ 的分歧群）．

证明　设 $G=\langle\sigma\rangle$，$\sigma^p=1$，$\pi\in\mathfrak{p}-\mathfrak{p}^2$，$\nu(\sigma)=\nu_\mathfrak{p}(\sigma(\pi)-\pi)$．由于 $|I_\mathfrak{p}|=e=p$，$e=e_0p$，$e_0=1$，而 $|I_\mathfrak{p}/V_1|\mid e_0$，从而 $G=$

$I_\mathfrak{p}=V_1$. 为证 $V_2=\{1\}$，我们只需再证 $\nu(\sigma)=2$ 即可。

由于 $\nu_\mathfrak{p}(\pi)=1$，而对每个 $a\in\mathbb{Q}$ 均有 $p|\nu_\mathfrak{p}(a)$，从而 $\pi\notin\mathbb{Q}$，因此 $K=\mathbb{Q}(\pi)$. π 的极小多项式为

$$f(x)=\prod_{i=0}^{p-1}(x-\sigma^i(\pi))=x^p+a_1x^{p-1}+\cdots+a_p\in\mathbb{Z}[x].$$

$$f'(\pi)=\sum_{i=1}^{p-1}(\pi-\sigma^i(\pi)).$$

由于 $\sigma^i(\pi)\in\sigma^i(\mathfrak{p})=\mathfrak{p}$，从而 $a_i\in\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$. 即 $p|a_i(1\leqslant i\leqslant p)$。另一方面，如果 $\nu_\mathfrak{p}(\sigma(\pi)-\pi)\geqslant a$，则

$$\nu_\mathfrak{p}(\sigma^{i+1}(\pi)-\sigma^i(\pi))\geqslant a,$$

从而

$$\nu_\mathfrak{p}(\sigma^j(\pi)-\pi)=\nu_\mathfrak{p}\left(\sum_{i=0}^{j-1}(\sigma^{i+1}(\pi)-\sigma^i(\pi))\right)\geqslant a\,(1\leqslant j\leqslant p-1).$$

由于 σ^j 也为 G 的生成元，从而由 $\nu_\mathfrak{p}(\sigma^j(\pi)-\pi)\geqslant a$ 也可推得

$$\nu_\mathfrak{p}(\sigma(\pi)-\pi)\geqslant a.$$

这就表明

$$\nu_\mathfrak{p}(\sigma^j(\pi)-\pi)=\nu_\mathfrak{p}(\sigma(\pi)-\pi)=\nu(\sigma)\quad(1\leqslant j\leqslant p-1).$$

因此 $\nu_\mathfrak{p}(f'(\pi))=(p-1)\nu(\sigma)$，但是

$$f'(\pi)=p\pi^{p-1}+(p-1)a_1\pi^{p-2}+\cdots+a_{p-1},$$

右边各项的 $\nu_\mathfrak{p}$ 值模 p 分别同余于 $p-1$，$p-2$，…，0. 于是这些项的 $\nu_\mathfrak{p}$ 值均不相等. 从而 $\nu_\mathfrak{p}(f'(\pi))$ 应当等于其中的最小者，特别地应当有 $\nu_\mathfrak{p}(f'(\pi))\leqslant\nu_\mathfrak{p}(p\pi^{p-1})=2p-1$，于是 $(p-1)\nu(\sigma)\leqslant 2p-1$. 由于 $p\geqslant 3$ 可知 $\nu(\sigma)\leqslant 2$. 另一方面，$\sigma\in G=V_1$，因此 $\nu(\sigma)=\nu_\mathfrak{p}(\sigma(\pi)-\pi)\geqslant 2$，这就证明了 $\nu(\sigma)=2$. 从而也证明了引理1. ▮

引理20 设 p 为奇素数，K 为 p^2 次 Abel 数域，并且只有 p 在 K 中分歧，则 K 必为循环域.

证明 令 $G=\mathrm{Gal}(K/\mathbb{Q})$，$\mathfrak{p}/p$，则 $|G|=p^2$，$e(\mathfrak{p}/p)=|I_\mathfrak{p}|$. 由于 $\mathfrak{p}$ 的惯性域 K_I 是 $\mathbb{Q}$ 的不分歧扩张，因此 $K_I=\mathbb{Q}$，于是 $|I_\mathfrak{p}|=p^2$. 从而 p 在 K_2 中完全分歧：$pO_K=\mathfrak{p}^{p^2}$，$N(\mathfrak{p})=p$。取 $\pi\in\mathfrak{p}-\mathfrak{p}^2$，并且令

$$G=I_{\mathfrak{p}}=V_1=\cdots=V_{i-1}\supsetneqq V_i\,(i\geqslant 2),$$

由于$|V_{i-1}/V_i|\,|N(\mathfrak{p})=p$，可知$V_i$为$p$阶循环群．设$K_0$为对应于$V_i$的子域，则$[K_0{:}\mathbb{Q}]=p$．如果$G$不是循环群，则$G$还有$p$阶循环子群$H\neq V_i$．设$K'$是对应于$H$的子域，则$[K'{:}\mathbb{Q}]=p$，$K'\neq K_0$．由于$p$在$K$中完全分歧，从而在$K'$中也完全分歧：$pO_{K'}=\mathfrak{p}'^p$，于是$\mathfrak{p}'O_K=\mathfrak{p}^p$．令

$$g(x)=\prod_{\tau\in H}(x-\tau(\pi))=x^p+a_1x^{p-1}+\cdots+a_p\in O_{K'}[x].$$

由于$\nu_{\mathfrak{p}}(-a_p)=\nu_{\mathfrak{p}}(\prod_{\tau\in H}\tau(\pi))=p$，从而$\nu_{\mathfrak{p}'}(a_p)=1$，即$a_p\in\mathfrak{p}'-\mathfrak{p}'^2$．对于$\sigma\in G$，$\gamma\equiv b_0+b_1a_p+b_2a_p^2+\cdots+b_ma_p^m\,(\mathrm{mod}\,\mathfrak{p}'^{m+1})$，$b_i\in\mathbb{Q}=K_I$，于是

$$\sigma(\gamma)-\gamma\equiv b_1(\sigma(a_p)-a_p)+\cdots+b_m(\sigma(a_p)^m-a_p^m)\,(\mathrm{mod}\,\mathfrak{p}'^{m+1}).$$

因此若$\nu_{\mathfrak{p}'}(\sigma(a_p)-a_p)\geqslant m+1$，则$\nu_{\mathfrak{p}'}(\sigma(\gamma)-\gamma)\geqslant m+1$．现在考虑等式

$$\begin{aligned}\sigma(g(\sigma^{-1}(\pi)))&=\sigma(g(\sigma^{-1}(\pi)))-g(\pi)\\&=(\sigma(a_1)-a_1)\pi^{p-1}+\cdots+(\sigma(a_p)-a_p),\end{aligned}\qquad(1)$$

如果$\sigma\in G-H$，则σH生成G/H．由引理1便知$\nu_{\mathfrak{p}'}(\sigma(a_p)-a_p)=2$，从而$\nu_{\mathfrak{p}}(\sigma(a_p)-a_p)=2p$，因此

$$\nu_{\mathfrak{p}}(\sigma(a_i)-a_i)\geqslant 2p\quad(1\leqslant i\leqslant p).$$

又由于$\pi\in\mathfrak{p}$，可知(1)式右边最后一项的$\nu_{\mathfrak{p}}$值最小．因此$\nu_{\mathfrak{p}}(\sigma(g(\sigma^{-1}(\pi))))=2p$．另一方面，

$$\sigma(g(\sigma^{-1}(\pi)))=\sigma(\prod_{\tau\in H}(\sigma^{-1}(\pi)-\tau(\pi)))=\prod_{\tau\in H}(\pi-\sigma\tau(\pi)).$$

记$\nu(\sigma\tau)=\nu_{\mathfrak{p}}(\sigma\tau(\pi)-\pi)$，于是

$$2p=\sum_{\tau\in H}\nu(\sigma\tau)\quad(\text{对于 }\sigma\in G-H).\qquad(2)$$

同样地，对于p次子域K_0，也有

$$2p=\sum_{\rho\in V_i}\nu(\sigma_0\rho)\quad(\text{对于}\sigma_0\in G-V_i).\qquad(3)$$

由于$H\cap V_i=\{1\}$，从而当$1\neq\tau\in H$时，$\tau\notin V_i$．因此$\nu(\tau)<i+1$．而当$1\neq\rho\in V_i$时，$\nu(\rho)\geqslant i+1$．因此$\sum\limits_{1\neq\tau\in H}\nu(\tau)<\sum\limits_{1\neq\rho\in V_i}\nu(\rho)$．

将 $\sum\limits_{1\neq\sigma\in G}\nu(\sigma)$ 减去此式两边，得到

$$\sum_{\sigma\in G-H}\nu(\sigma)>\sum_{\sigma'\in G-V_i}\nu(\sigma'), \tag{4}$$

可是由(2)和(3)式推得(4)式两边均应当为 $(p-1)\cdot 2p$，这一矛盾表明 $K/\mathbb{Q}$ 必然是循环扩张. ▌

现在由引理 1 和引理 2 证明(三)，我们分 $p\geqslant 3$ 和 $p=2$ 两种情形：

(A) 对于 $p\geqslant 3$，令 K 是 p^v 次循环域，并且只有 p 在 K 中分歧. 令 $L=F_{p^v}K$，则 L 为 p 幂次的 Abel 扩张，并且也只有 p 在 L 中分歧. 如果 $L/\mathbb{Q}$ 不是循环扩张，则 $G=\mathrm{Gal}(L/\mathbb{Q})$ 有一个子群 N，使得 G/N 为 (p, p) 型 Abel 群. 设 N 对应于子域 L'，则 $L'/\mathbb{Q}$ 为 (p, p) 型扩张，并且只有 p 在 L' 中分歧，根据引理 2 知这不可能. 从而 L/K 必是循环扩张. 于是 L 只有一个 p^v 次循环子域. 但是 F_{p^v} 和 K 均是这样的子域，这就表明 $K=F_{p^v}$，即 K 是分圆域的子域.

(B) 对于 $p=2$. 令 K 为 2^v 次循环域($V\geqslant 2$)，并且只有 2 在 K 中分歧.

如果 K 为实域，考虑 $L=F_{2^v}K$. 假如 L 不是循环域，则与 $p\geqslant 3$ 的情形一样可知 L 有 $(2, 2)$ 型的子域 L'，并且只有 2 在 L' 中分歧，从而 L' 有 $\geqslant 2$ 个不同的实二次域，使得 2 在其中均分歧. 但是易知这样的实二次域只有 $\mathbb{Q}(\sqrt{2})$. 这一矛盾表明 L 为循环域，然后与 $p\geqslant 3$ 情形一样推得 $K=F_{2^v}$，即 K 是分圆域的子域.

最后，如果 K 为虚域. 令 K_0 是 K 的极大实子域，则 K_0 为 2^{v-1} 次循环域(因为若 $K=\mathbb{Q}(\omega)$，则 $\omega\notin\mathbb{R}$. 从而 $K_0=\mathbb{Q}(\omega+\omega^{-1})$，而 $[K:K_0]=2$)，并且只有 2 在 K_0 中分歧. 由上述知 $\mathbb{Q}(\sqrt{2})\subseteq K_0$. 而 K 中只有一个二次子域，从而 $\mathbb{Q}(\sqrt{-1})\nsubseteq K$. 令 $L'=K\cdot\mathbb{Q}(\sqrt{-1})$. 则 L' 为 2^{v+1} 次 Abel 虚域，并且只有 2 在 L' 中分歧. 从而它的极大实子域 L_0' 为 2^v 次 Abel 域，并且只有 2 在 L_0' 中分歧. 于是由上一段的推理可知 L_0' 为循环域，从而 L_0' 为

分圆域的子域，从而 $L'=L_0'\mathbb{Q}(\sqrt{-1})$ 也为分圆域的子域．由于 $K\subseteq L'$，从而 K 也是分圆域的子域．这就证明了(三)，从而也同时完成了 Kronecker-Weber 定理的证明． ▌

注记 令 $\mathbb{Q}_{ab}=\bigcup_{n\geq 2}\mathbb{Q}(\zeta_n)$，这是 $\mathbb{Q}$ 的无限(次)扩域．而 Kronecker-Weber 定理可以叙述为：每个Abel数域均是 $\mathbb{Q}_{ab}$ 的子域．所以 $\mathbb{Q}_{ab}$ 叫作是有理数域的极大 Abel 扩张．$\mathbb{Q}_{ab}$ 是将复值周期函数 $e^{2\pi ix}$ 在所有有理点 $x\in\mathbb{Q}$ 处的值 $\{e^{2\pi ix}|x\in\mathbb{Q}\}$ 添加到 $\mathbb{Q}$ 之上而得到的域．Kronecker进而猜想，对于虚二次域 $K=\mathbb{Q}(\sqrt{-d})$ $(d>0)$，K 的极大 Abel 扩张是将某些复值双周期函数——椭圆模函数在全部有理点处的值添加到 K 上而得到的域．这就是所谓的"Kronecker 青春之梦"(Jugendfraum)．在 1920 年高木贞治创建了类域论之后，人们终于证明了这一猜想．但是对于其他数域 K(甚至对实二次域)，K 的极大 Abel 扩张究竟是什么？目前还不清楚．这是一个相当难的代数数论问题．

4.4 Abel 数域的导子和互反律

在本书的第二部分大家会看到，Kronecker-Weber 定理对于 Abel 数域的研究起着重要的作用．现在我们只谈谈此定理对于 Abel 数域中素理想分解规律所起的作用，这就是所谓 Abel 数域中的互反律．

设 K 为 Abel 数域．根据 Kronecker-Weber 定理，K 是某个分圆域的子域．如果 $K\subseteq\mathbb{Q}(\zeta_m)$，$K\subseteq\mathbb{Q}(\zeta_n)$，则

$$K\subseteq\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{(m,n)}).$$

这就表明存在一个最小的分圆域 $\mathbb{Q}(\zeta_m)$ $(m\not\equiv 2\pmod 4)$，使得 $K\subseteq\mathbb{Q}(\zeta_m)$．

定义 设 K 为 Abel 数域．若 $\mathbb{Q}(\zeta_m)$ $(m\not\equiv 2\pmod 4)$ 为包含 K 的最小分圆域，我们称 m 为 Abel 数域 K 的导子(conductor, führer)，并且表示成 $\mathfrak{f}(K)$．

定义 6 对于每个 n 次伽罗华数域 K，如果素数 p 在 K 中

的分解为 $pO_K=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^e$，$efg=n$，我们称 p 在 K 中的分解型式为 (e, f, g)。如果 p 在 K 中不分歧，即 $e=1$，我们也称 p 在 K 中的分解型式为 (f, g)。

定理 20（Abel 数域中的互反律） 设 K 是 Abel 数域，$\mathfrak{f}(K)$ 为它的导子，p 和 p' 是两个素数，并且

$$(p, \mathfrak{f}(K))=(p', \mathfrak{f}(K))=1.$$

如果 $p\equiv p'(\bmod \mathfrak{f}(K))$，则 p 和 p' 在 K 中有相同的分解型式。

证明 根据定义，$K\subseteq L=\mathbb{Q}(\zeta_{\mathfrak{f}(K)})$。令 $G=\mathrm{Gal}(L/\mathbb{Q})$，则 G 正则同构于 $(\mathbb{Z}/\mathfrak{f}(K)\mathbb{Z})^\times$：

$$\varphi:\ \mathrm{Gal}(L/\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}/\mathfrak{f}(K)\mathbb{Z})^\times,\ \sigma_a\mapsto a(\bmod \mathfrak{f}(K)),$$

$$(a, \mathfrak{f}(K))=1,$$

其中 σ_a 表示 L 中自同构 $\zeta_{\mathfrak{f}(K)}\mapsto\zeta_{\mathfrak{f}(K)}^a$。令 N 为 K 的固定子群，则 $\mathrm{Gal}(K/\mathbb{Q})\cong G/N\cong(\mathbb{Z}/\mathfrak{f}(K)\mathbb{Z})^\times/\varphi(N)$。如果 $(p, \mathfrak{f}(K))=1$，则素数 p 在 L 中从而也在 K 中不分歧。于是

$$pO_K=\mathfrak{p}_1\cdots\mathfrak{p}_g,\ f=f(\mathfrak{p}_i|p),\ fg=n,\ I_p=\{1\}.$$

D_p 为 f 阶循环群并且 D_p 由 Frobenius 自同构 $\tau_p=\left(\frac{K/\mathbb{Q}}{p}\right)$所生成。我们已经证明过，$\sigma_p$ 是 Frobenius 自同构$\left(\frac{L/\mathbb{Q}}{p}\right)$，并且 $\sigma_p|K=\tau_p$。由于 τ_p 的阶为 f，于是 f 是满足 $\sigma_p{}^f|K=(\sigma_p|_K)^f=1\in\mathrm{Gal}\,(K/\mathbb{Q})$ 的最小正整数。利用同构 φ 便知 f 是满足 $\bar{p}^f\in\varphi(N)$的最小正整数，其中 $\bar{p}$ 表示 p 的模 $\mathfrak{f}(K)$ 同余类。令

$$\varphi(N)=\{\bar{a}_1, \cdots, \bar{a}_t\},\ t=|N|=[L:K],\ a_i\in\mathbb{Z},$$

则 f 即是使得

$$p^f\equiv a(\bmod f(K))\text{对于某个 } a\in\{a_1, \cdots, a_t\}$$

成立的最小正整数 f。从这一种刻划方式不难看出，f 只与 p 的模 $\mathfrak{f}(K)$ 同余类有关，因此当 $p\equiv p'(\bmod \mathfrak{f}(K))$ 时，p 和 p' 有相同的 f，从而有相同的分解型式 (f, g)，$fg=n$。 ∎

例 分圆域 $L=\mathbb{Q}(\omega)$，$\omega=\zeta_{17}$ 是 16 次循环域，

$$G=\mathrm{Gal}(L/\mathbb{Q})=\langle\sigma_3\rangle.$$

令 K 为 L 的唯一的 4 次循环子域，则 K 的固定子群为

$$N=\{\sigma_1,\ \sigma_{3^4},\ \sigma_{3^8},\ \sigma_{3^{12}}\}=\{\sigma_1,\ \sigma_{-4},\ \sigma_{-1},\ \sigma_4\}.$$

于是由伽罗华理论不难看出

$$K=\mathbb{Q}(\varepsilon),\ \varepsilon=\omega+\omega^{-1}+\omega^4+\omega^{-4}.$$

当素数 $p\neq 17$ 时，p 在 K 中不分歧．根据上述定理的证明即知：

(i) p 在 K 中惯性 $\Leftrightarrow f=4\Leftrightarrow$ 满足 $p^f\equiv 3^0,\ 3^4,\ 3^8,\ 3^{12}\pmod{17}$ 的最小正整数 f 为 $4\Leftrightarrow p\equiv 3^{\pm1},\ 3^{\pm3},\ 3^{\pm5},\ 3^{\pm7}\equiv\pm3,\ \pm5,\ \pm6,\ \pm7\pmod{17}$．

(ii) $pO_K=\mathfrak{p}_1\mathfrak{p}_2\Leftrightarrow f=2\Leftrightarrow$ 满足 $p^f\equiv 3^0,\ 3^4,\ 3^8,\ 3^{12}\pmod{17}$ 的最小正整数 f 为 $2\Leftrightarrow p\equiv 3^{\pm2},\ 3^{\pm6}\equiv\pm2,\ \pm9\pmod{17}$．

(iii) $pO_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$（完全分裂）$\Leftrightarrow p\equiv 3^0,\ 3^4,\ 3^8,\ 3^{12}\equiv\pm1,\ \pm4\pmod{17}$．

注记

1．定理 20 和上面的例子表明，在 Abel 数域 K 中，具有同样分解型式的素数集合是公差为 $\mathfrak{f}(K)$ 的一些算术级数之并．这就自然产生如下的问题：对于每个正整数 k 和与 k 互素的整数 l，算术级数 $l+nk\,(n\in\mathbb{Z})$ 中是否存在着无限多个素数？利用解析工具，我们在本书第二部分将要证明答案是肯定的，即当 $(k,\ l)=1$ 时，存在无限多个素数 p 使得 $p\equiv l\pmod{k}$．而且，对于 $\varphi(k)$ 个不同的 l 值，$(k,\ l)=1$，全体素数在相应的公差为 k 的 $\varphi(k)$ 个不同的算术级数中分布是均匀的．确切地说，如果以 $\pi(x)$ 表示不超过 x 的素数的个数，以 $\pi(x,\ l,\ k)$ 表示算术级数 $l+nk\,(n\in\mathbb{Z})$ 中不超过 x 的素数的个数，则对于每个 l，$(l,\ k)=1$，均有

$$\lim_{x\to\infty}\frac{\pi(x,\ l,\ k)}{\pi(x)}=\frac{1}{\varphi(k)}.$$

比如对于上面的例子，即对于 4 次循环域 $\mathbb{Q}(\omega+\omega^{-1}+\omega^4+\omega^{-4})$，$\omega=\zeta_{17}$，则在 K 中惯性的素数，在 K 中完全分裂的素数，以及在 K 中分解成两个素理想之积的素数，其在全体素数中所占的比例为 $\frac{8}{16}:\frac{4}{16}:\frac{4}{16}=\frac{1}{2}:\frac{1}{4}:\frac{1}{4}$．

2．二次域中的互反律可以从二次互反律（定理16）推出．

(习题 1). 对于任意的数域扩张 L/K 应当有什么样的一般互反律? 这是 Hilbert 著名的 23 个问题当中的一个. 随着类域论的建立, Artin 和 Hasse 等人在一般互反律方面作了许多深刻的工作. Artin 将一般互反律看作是类域论的核心. 这些问题在作为引论的本书中就不作进一步介绍了.

习　　题

1. 试用二次互反律(定理16)证明下列二次域中素理想分解的互反律: 设 $K=\mathbb{Q}(\sqrt{d})$, p 和 p' 为素数, 并且 $(p, d(K))=(p', d(K))=1$. 则当 $p\equiv p' \pmod{d(K)}$ 时, p 和 p' 在 K 中或者均是惯性, 或者均是完全分裂.
2. 设 p 为素数, $n|(p-1)$, K 是分圆域 $\mathbb{Q}(\zeta_p)$的唯一 n 次子域, 对于每个素数 $q\neq p$, 设 q 在 K 中素理想分解型式为(f, g), $fg=n$, 求证 f 是使 q^f为模 p 的 n 次剩余的最小正整数 (a 叫作是模 p 的 n 次剩余, 是指有 $b\in\mathbb{Z}$, 使得 $a\equiv b^n \pmod{p}$).
3. 设 $f(x)=x^3+px+q$ 是 $\mathbb{Q}[x]$ 中三次不可约多项式, α 是 $f(x)$ 的一个根, $K=\mathbb{Q}(\alpha)$.

   (a) 求证 K 是三次循环域的充要条件是 $-4p^3-27q^2$ 为某个有理数的平方.

   (b) 设 α 为 $f(x)=x^3-3x+1$ 的一个根. 求证 $K=\mathbb{Q}(\alpha)$ 是三次循环域. 试问域 K 的导子 $\mathfrak{f}(K)$是多少?
4. 求 Abel 域 $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ 和 $\mathbb{Q}(\sqrt{-1}, \sqrt{7})$的导子.
5. 设 $F(x)$是 $\mathbb{Z}[x]$中的 n 次首 1 多项式, α 是 $F(x)$ 的一个根. 如果 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 为伽罗华扩张, 我们称 $F(x)$ 是 $\mathbb{Q}$ 上的正规多项式. 又若 $\mathbb{Q}(\alpha)$是 Abel 数域, 则称 $F(x)$是 $\mathbb{Q}$ 上的 **Abel 多项式**. 求证:

   (a) 如果 $F(x)$是 $\mathbb{Q}$ 上的正规多项式, 则存在正整数 N, 使得对于每个素数 $p>N$, $F(x)$在有限域 $\mathbb{F}_p$ 上均分解成次数相同的一些不可约多项式之积. 换句话说, 当 $p>N$ 时

   $$F(x)\equiv F_1(x)F_2(x)\cdots F_g(x) \pmod{p},$$

   其中 $F_i(x)(1\leqslant i\leqslant g)$均是 $\mathbb{F}_p[x]$中次数为 $f=n/g$ 的不可约多项式. 这时, 我们称(f, g)为 $F(x)$在有限域 $\mathbb{F}_p$ 上的分解型式.

   (b) 如果 $F(x)$是 $\mathbb{Q}$ 上的 Abel 多项式, 则存在正整数 N 和 n, 使得对于

任意两个素数 p_1 和 p_2，只要 $p_1>N$，$p_2>N$，并且 $p_1\equiv p_2 \pmod n$，那末 $F(x)$ 在域 $\mathbb{F}_{p_1}$ 和 $\mathbb{F}_{p_2}$ 中就有同样的分解型式。

6. (a) 求证 $f(x)=x^3+x^2-2x-1$ 是 $\mathbb{Q}$ 上的 Abel 多项式，并且上题(b)中的 N 和 n 均可取为 7；

(b) 求证：当素数 $p\equiv\pm1 \pmod 7$ 时，$f(x)$ 在域 $\mathbb{F}_p$ 中有三个不同的根；当素数 $p\equiv\pm2,\ \pm3 \pmod 7$ 时，$f(x)$ 在 $\mathbb{F}_p$ 中为不可约多项式；最后，$f(x)$ 在 $\mathbb{F}_7$ 中有一个重数为 3 的根。

第三章　理想类群和单位群

§1　类群和类数

这一节的内容是接过§3中的话题讲下去. 我们在§3中证明了，数域K的全部分式理想形成群$I(K)$，其中的主分式理想全体是它的一个子群$P(K)$，并且证明了以下三件事情是彼此等价的：

(1) $I(K)=P(K)$，即K中每个分式理想均为主分式理想；

(2) 整数环O_K为主理想整环，即O_K中每个理想均是主理想；

(3) O_K是唯一因子分解整环.

我们在本书绪言中也说过，从Kummer时代起人们就发现，存在着数域K，其整数环O_K不是唯一因子分解整环，即$I(K)\supsetneqq P(K)$. 这种域的最简单例子是实二次域$\mathbb{Q}(\sqrt{10})$和虚二次域$\mathbb{Q}(\sqrt{-5})$. Kummer研究Fermat问题时，所关心的是分圆域$\mathbb{Q}(\zeta_p)$的整数环$\mathbb{Z}[\zeta_p]$. 他发现当$3\leqslant p\leqslant 19$时，$\mathbb{Z}[\zeta_p]$是唯一因子分解整环，而$\mathbb{Z}[\zeta_{23}]$则不是. 对于O_K不为唯一因子分解整环即$I(K)\supsetneqq P(K)$的情形，人们自然想到用商群$I(K)/P(K)$的大小来衡量O_K与唯一因子分解整环相距多远. 这就导致对商群$I(K)/P(K)$的研究.

定义1　设$\mathfrak{A}$和$\mathfrak{B}$是数域K中的两个分式理想. 如果$\mathfrak{A}\mathfrak{B}^{-1}\in P(K)$，即$\mathfrak{A}\mathfrak{B}^{-1}$是主分式理想，我们称$\mathfrak{A}$和$\mathfrak{B}$是等价的，表示成$\mathfrak{A}\sim\mathfrak{B}$.

分式理想的等价显然是一个等价关系. 由此分成的(分式)理想等价类显然是Abel群$I(K)$对于子群$P(K)$的陪集，从而可看成是商群$I(K)/P(K)$中的元素. $P(K)$就是主(分式)理想等价类. 因此，我们将商群$C(K)=I(K)/P(K)$称作是数域K的理想类群，简称作类群，而$C(K)$中的每个元素叫作是K中的一个理想类.

$C(K)$显然是 Abel 群. Dirichlet 给出关于理想类群的奠基性结果: 对于每个数域 K, $C(K)$是有限 Abel 群. 于是$C(K)$的阶 $h(K)=|C(K)|$是有限的, $h(K)$叫作是数域K的理想类数,简称作类数. 因此 Dirichlet 的上述结果也叫作是类数有限性定理. 而对于每个数域K, O_K 为主理想整环(或唯一因子分解整环)的充要条件是K的类数$h(K)$为1. 从那时起, 对于数域K的类群$C(K)$和类数$h(K)$的研究, 就成了代数数论的中心课题之一.

本节的主要目标是证明 Dirichlet 类数有限性定理. 我们也具体计算一些数域的类群和类数. 首先需要作一些准备工作.

1.1 $\mathbb{R}^n$ 中的格, Minkowski 定理

定义 2 加法群$\mathbb{R}^n$的子集H叫作$\mathbb{R}^n$的一个格, 是指存在n维实向量空间$\mathbb{R}^n$中的一组基$\{\alpha_1, \cdots, \alpha_n\}$, 使得 $H=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$. 于是, $\mathbb{R}^n$中每个格H均是秩n的自由 Abel 加法群. 而$\{\alpha_1, \cdots, \alpha_n\}$是加法群$H$的一组基.

设H是$\mathbb{R}^n$中一个格, $\{\alpha_1, \cdots, \alpha_n\}$是$H$的一组基. 定义

$$P(\alpha_1, \cdots, \alpha_n)=\left\{\sum_{i=1}^{n} a_i\alpha_i \,\middle|\, 0\leqslant a_i<1\right\},$$

这是$\mathbb{R}^n$中的一个平行多面体. 由于$\{\alpha_1, \cdots, \alpha_n\}$也是实向量空间$\mathbb{R}^n$的一组基,从而$\mathbb{R}^n$中每个元素(即向量)均可唯一地表示成$\alpha=r_1\alpha_1+\cdots+r_n\alpha_n$, $r_i\in\mathbb{R}$. 以$[r]$表示实数r的整数部分,则$0\leqslant\{r\}=r-[r]<1$,并且$\alpha=h+f$,其中

$$h=\sum_{i=1}^{n}[r_i]\alpha_i\in H,\ f=\sum_{i=1}^{n}\{r_i\}\alpha_i\in P(\alpha_1, \cdots, \alpha_n).$$

换句话说, $\mathbb{R}^n$中每个元素均属于$f+H$, 其中$f\in P(\alpha_1, \cdots, \alpha_n)$. 另一方面, 对于$P(\alpha_1, \cdots, \alpha_n)$中两个不同的元素$f_1$和$f_2$, 显然$f_1-f_2\notin H$. 这就表明$P(\alpha_1, \cdots, \alpha_n)$是加法商群$\mathbb{R}^n/H$中诸陪集的完全代表元系.

取$e_1=(1, 0, \cdots, 0)$, $e_2=(0, 1, 0, \cdots, 0)$, $\cdots$, $e_n=(0, \cdots,$

$0, 1)$为实向量空间 $\mathbb{R}^n$ 的标准基. 设$\alpha_i=\sum_{j=1}^{n} r_{ij}e_j$, $r_{ij}\in\mathbb{R}$. μ 表示 $\mathbb{R}^n$ 上的 Lebesque 测度. 熟知 $\mu(P(\alpha_1, \cdots, \alpha_n))=|\det(r_{ij})|$. 如果$\{\alpha_1', \cdots, \alpha_n'\}$是格 H 的另一组基, $\alpha_i'=\sum_{j=1}^{n} a_{ij}\alpha_j$, 则 $a_{ij}\in\mathbb{Z}$ 并且 $\det(a_{ij})=\pm1$. 于是

$$\mu(P(\alpha_1', \cdots, \alpha_n'))=|\det(r_{ij})\cdot\det(a_{ij})|$$
$$=|\det(r_{ij})|=\mu(P(\alpha_1, \cdots, \alpha_n)).$$

这就表明 $\mu(P(\alpha_1, \cdots, \alpha_n))$与基$\{\alpha_1, \cdots, \alpha_n\}$的选取无关, 即是格 H 本身的特性. 我们将它叫作是格 H 的体积, 表示成 $V(H)$. 粗糙地说, 格 H 在 $\mathbb{R}^n$ 中分布愈稀疏, 则格 H 的体积(即平行多面体 $P(\alpha_1, \cdots, \alpha_n)$的测度)也愈大.

引理 1 设 H 和 H' 均是 $\mathbb{R}^n$ 中的格, 并且 $H\supseteq H'$. 则加法商群 H/H' 是有限群, 并且$|H/H'|=V(H')/V(H)$.

证明 由于 H' 和 H 均是秩 n 的自由 Abel 群, 从附录 B, (1)即知存在 H 的一组基$\{\alpha_1, \cdots, \alpha_n\}$, 使得 $H'=\mathbb{Z}d_1\alpha_1\oplus\cdots\oplus\mathbb{Z}d_n\alpha_n$. $d_i\in\mathbb{Z}-\{0\}$. 于是

$$H/H'=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n/\mathbb{Z}d_1\alpha_1\oplus\cdots\oplus\mathbb{Z}d_n\alpha_n$$
$$\cong\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_n\mathbb{Z}.$$

从而$|H/H'|=|d_1\cdots d_n|$. 另一方面, 如果 $\alpha_i=\sum_{j=1}^{n} r_{ij}e_j$, 则

$$V(H')=|\det(d_ir_{ij})|=|d_1\cdots d_n|\cdot|\det(r_{ij})|$$
$$=|d_1\cdots d_n|\cdot V(H).$$

由此即得引理. ▌

定义 3 $\mathbb{R}^n$ 的加法子群 H 叫作是离散的, 是指对于 $\mathbb{R}^n$ 的每个有界子集 K, $K\cap H$ 均是有限集合.

引理 2 (a) $\mathbb{R}^n$ 中每个格 H 均是 $\mathbb{R}^n$ 的离散子群.

(b) $\mathbb{R}^n$ 中的每个离散子群 D 必是 $\mathbb{R}^n$ 的某个 r 维子空间($0\leqslant r\leqslant n$)中的格.

证明 (a) 设 H 为 $\mathbb{R}^n$ 的格, $\{\alpha_1, \cdots, \alpha_n\}$是 H 的一组基, 则$\{\alpha_1, \cdots, \alpha_n\}$也是实向量空间 $\mathbb{R}^n$ 的一组基. 如果 K 是 $\mathbb{R}^n$ 中的有

界子集，则 K 中元素对于基$\{\alpha_1, \cdots, \alpha_n\}$的坐标均是有界的，即存在某个常数 M，使得当 $\alpha=\sum_{i=1}^{n} r_i\alpha_i \in K$, $r_i \in \mathbb{R}$ 时，必然 $|r_i| \leqslant M$ $(1\leqslant i\leqslant n)$. 如果 $\alpha\in K\cap H$，则 $r_i \in \mathbb{Z}$, $|r_i|\leqslant M$. 这只有有限多个可能，从而 $K\cap H$ 为有限集合，于是 H 是 $\mathbb{R}^n$ 的离散子群.

(b) 设 D 是 $\mathbb{R}^n$ 的离散子群，$\{\alpha_1, \cdots, \alpha_r\}$为 D 中极大 $\mathbb{R}$-线性无关子集合，则 $0\leqslant r\leqslant n$. 由于平行多面体 $P=P(\alpha_1, \cdots, \alpha_r)$ 为 $\mathbb{R}^n$ 的有界子集合，从而 $P\cap D$ 为有限集合. 由$\{\alpha_1, \cdots, \alpha_r\}$的极大性可知每个 $x\in D$ 均可表为 $x=\sum_{i=1}^{r}\lambda_i\alpha_i$, $\lambda_i\in\mathbb{R}$. 对于每个 $j\in\mathbb{Z}$，令

$$x_j=jx-\sum_{i=1}^{r}[j\lambda_i]\alpha_i=\sum_{i=1}^{r}\{j\lambda_i\}\alpha_i\in D\cap P.$$

而 $x=x_1+\sum_{i=1}^{r}[\lambda_i]\alpha_i$, $x_1\in D\cap P$，从而 D 是由有限集合 $(D\cap P)\cup\{\alpha_1, \cdots, \alpha_n\}$生成的子群，即 D 为有限生成 Abel 群. 另一方面，由于 $D\cap P$ 有限而 $\mathbb{Z}$ 无限，可知存在两个不同的整数 j 和 k，使得 $x_j=x_k$，即 $(j-k)\lambda_i=[j\lambda_i]-[k\lambda_i]\in\mathbb{Z}$，于是 $\lambda_i\in\mathbb{Q}(1\leqslant i\leqslant r)$. 由于 D 是有限生成的，并且每个生成元均为$\{\alpha_1, \cdots, \alpha_r\}$的 $\mathbb{Q}$-线性组合，乘以诸系数的公分母 $d(\neq 0)$之后，可知 $dD\subseteq\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_r$. 即 dD 为秩 r 的自由 Abel 群 $\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_r$ 的子群. 根据附录 B，(1) 可知 dD 为秩 $\leqslant r$ 的自由 Abel 群. 但是 $r\leqslant \operatorname{rank} D=\operatorname{rank} dD\leqslant r$，因此 dD 的秩为 r，于是 $dD=\mathbb{Z}f_1\oplus\cdots\oplus\mathbb{Z}f_r$，而 $D=\mathbb{Z}f_1/d\oplus\cdots\oplus\mathbb{Z}f_r/d$. 这就表明 D 是 $\mathbb{R}^n$ 中由向量 f_i/d $(1\leqslant i\leqslant r)$ 张成的 r 维子空间中的格. ▮

定义 4 $\mathbb{R}^n$ 中子集合 S 叫作是凸集合，是指

$$x,\ y\in S\Rightarrow\frac{1}{2}(x+y)\in S.$$

S 叫作是关于原点对称的，是指 $x\in S\Rightarrow -x\in S$.

定理 1 (Minkowski) 设 H 为 $\mathbb{R}^n$ 中的格，S 是 $\mathbb{R}^n$ 中的 Lebesque可测子集合(测度表示成 $\mu(S)$).

(a) 如果 $\mu(S)>V(H)$，则存在 $s, s'\in S$, $s\neq s'$，使得 $s-s'\in$

H;

(b) 如果 S 又为关于原点对称的凸集，则当 $\mu(S)>2^nV(H)$ 时，$S\cap H$ 中有非零向量；

(c) 如果 S 为关于原点对称的紧凸集，则当 $\mu(S)\geqslant 2^nV(H)$ 时，$S\cap H$ 中有非零向量。

证明 (a) 取 $\alpha_1, \cdots, \alpha_n$ 为格 H 的一组基。$P=P(\alpha_1, \cdots, \alpha_n)$ 是上面定义的平行多面体，则 $\{h+P \mid h\in H\}$ 是一些两两非交的集合，它们的并集为 $\mathbb{R}^n$（这是由于 P 是 $\mathbb{R}^n/H$ 的诸陪集完全代表元系）。从而 $\{S\cap(h+P) \mid h\in H\}$ 也是一些两两非交的集合，并且它们的并集为 S。因此

$$\mu(S)=\sum_{h\in H}\mu(S\cap(h+P))=\sum_{h\in H}\mu((-h+S)\cap P).$$

如果对于 H 中任意两个不同的元素 h 和 h'，$(-h+S)\cap P$ 与 $(-h'+S)\cap P$ 均是非交的，则

$$\mu(S)=\sum_{h\in H}\mu((-h+S)\cap P)\leqslant\mu(P)=V(H),$$

这就与假设 $\mu(S)>V(H)$ 相矛盾，所以存在 $h, h'\in H$, $h\neq h'$，使得 $(-h+S)\cap P$ 与 $(-h'+S)\cap P$ 有公共元素 x，即

$$x=-h+s=-h'+s', \quad s, s'\in S.$$

而 $0\neq h-h'=s-s'\in H$。

(b) 令 $S'=\frac{1}{2}S$，则 $\mu(S')=\frac{1}{2^n}\mu(S)>V(H)$。由 (a) 知有 $x, y\in S'$, $x\neq y$，使得 $x-y\in H$。于是 $2x, -2y\in S$，从而

$$x-y=\frac{1}{2}(2x+(-2y))\in S,$$

即

$$0\neq x-y\in S\cap H.$$

(c) 取 $S_m=\left(1+\frac{1}{m}\right)S$。则 S_m 与 S 一样是关于原点对称的凸集，而 $\mu(S_m)=\left(1+\frac{1}{m}\right)^n\mu(S)>2^n\cdot V(H)$（当 $m\geqslant 1$ 时）。于是由 (b) 知有 $0\neq h_m\in S_m\cap H$。由于 $\{h_n \mid n\geqslant 1\}$ 是紧集 $S_1=2S$ 中的序列，从而有一个子序列收敛于某点 $h\in\mathbb{R}^n$ 由于 $\lim\limits_{m\to\infty}S_m=S$，而

S 为紧集，可知 $h\in S$. 又由于 H 是 $\mathbb{R}^n$ 的离散子群，易知 H 中非零子序列 $\{h_m|m\geqslant 1\}$ 的极限 $h\in H$ 并且 $h\neq 0$. 于是 $0\neq h\in S\cap H$. ∎

注记 Minkowski 定理是说，一个比较规则的图形当体积足够大时，必然包含格 H 中的一个点 $x\neq 0$. 特别当 $H=\mathbb{Z}^n$ 时，这就是通常所谓整点问题. 研究 $\mathbb{R}^n$ 中某个几何图形中整点的存在性以及估计整点个数，这是数论的一个分支——"数的几何"中的一个主要课题，而 Minkowski 定理则是这一分支的奠基性定理.

1.2 类数有限性定理

现在我们由 Minkowski 定理得到 Dirichlet 的类数有限性定理以及其他一些有益的结果. 方法是：通过 n 次数域 K 到 $\mathbb{C}$ 中的 n 个嵌入将 K 的每个理想对应于 $\mathbb{R}^n$ 中的一个格.

我们在第一章中讲过，每个 n 次数域 K 到 $\mathbb{C}$ 中有 r_1 个实嵌入 σ_i: $K\to\mathbb{R}$ $(1\leqslant i\leqslant r_1)$ 和 r_2 对复嵌入 $\sigma_{r_1+j}=\overline{\sigma}_{r_1+r_2+j}$: $K\to\mathbb{C}$ $(1\leqslant j\leqslant r_2)$，$r_1+2r_2=n$. 由此得到映射

$$\sigma: K\to\mathbb{R}^n,\ \sigma(\alpha)=(\sigma_1(\alpha),\ \cdots,\ \sigma_{r_1}(\alpha),\ \mathrm{Re}(\sigma_{r_1+1}(\alpha)),\ \cdots,\ \mathrm{Re}(\sigma_{r_1+r_2}(\alpha)),\ \mathrm{Im}(\sigma_{r_1+1}(\alpha)),\ \cdots,\ \mathrm{Im}(\sigma_{r_1+r_2}(\alpha))),$$

其中 $\mathrm{Re}(\gamma)$，$\mathrm{Im}(\gamma)$ 分别表示复数 γ 的实部和虚部. σ 显然是加法群的同态. 进而，由于每个 σ_i 均是单同态，可知 σ 是单同态，即 σ 为嵌入. 我们称 σ 为 K 到 $\mathbb{R}^n$ 中的正则嵌入.

引理 3 设 $\mathfrak{a}$ 为 n 次数域 K 中的非零整理想. 则 $\sigma(\mathfrak{a})$ 是 $\mathbb{R}^n$ 中的格，并且 $V(\sigma(\mathfrak{a}))=2^{-r_2}N(\mathfrak{a})\,|d(K)|^{1/2}$.

证明 我们在第一章中证明了整理想 $\mathfrak{a}$ 的加法群是秩 n 的自由 Abel 群. 即 $\mathfrak{a}=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$. 取 $e_1,\ \cdots,\ e_n$ 为 $\mathbb{R}^n$ 的标准基，则 $\sigma(\alpha_i)=\sum\limits_{j=1}^{n}x_{ij}e_j$，其中

$$x_{ij}=\begin{cases}\sigma_j(\alpha_i),\ 1\leqslant j\leqslant r_1;\\ \mathrm{Re}(\sigma_j(\alpha_i)),\ r_1+1\leqslant j\leqslant r_1+r_2;\\ \mathrm{Im}(\sigma_j(\alpha_i)),\ r_1+r_2+1\leqslant j\leqslant n.\end{cases}$$

于是 $\sigma(\mathfrak{a})=\mathbb{Z}\sigma(\alpha_1)+\cdots+\mathbb{Z}\sigma(\alpha_n)$. 并且

$$
\begin{aligned}
V(\sigma(\mathfrak{a})) &= |\det(x_{ij})| = 2^{-r_2}|\det(\sigma_j(\alpha_i))| \\
&= 2^{-r_2}|d_K(\alpha_1, \cdots, \alpha_n)|^{1/2} = 2^{-r_2}N(\mathfrak{a})|d(K)|^{1/2}.
\end{aligned}
$$

由于上式右边不为 0, 即 $\det(x_{ij})\neq 0$, 这就表明 $\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$ 是 $\mathbb{R}$-线性无关的, 从而 $\sigma(\mathfrak{a})=\mathbb{Z}\sigma(\alpha_1)\oplus\cdots\oplus\mathbb{Z}\sigma(\alpha_n)$ 为 $\mathbb{R}^n$ 中的格. ▮

引理 4 设 $\mathfrak{a}$ 是数域 K 中的非零整理想,

$$[K:\mathbb{Q}]=n=r_1+2r_2.$$

则

(a) 存在 $0\neq x\in\mathfrak{a}$, 使得

$$|N_{K/\mathbb{Q}}(x)|\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}N(\mathfrak{a}).$$

(b) K 的每个理想类 C 中均有整理想 $\mathfrak{B}$, 使得

$$N(\mathfrak{B})\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}.$$

证明 (a) 对于 $y=(y_1, \cdots, y_n)\in\mathbb{R}^n$, 定义

$$\lambda(y)=\sum_{i=1}^{r_1}|y_i|+2\sum_{j=1}^{r_2}(y_{r_1+j}^2+y_{r_1+r_2+j}^2)^{1/2}.$$

对于 $t>0$, 定义 $\mathbb{R}^n$ 中集合 $B_t=\{y=(y_1, \cdots, y_n)\in\mathbb{R}^n|\lambda(y)\leqslant t\}$. 易知 B_t 是关于原点对称的紧凸集, 由多重定积分可算出

$$\mu(B_t)=\int\cdots\int_{\lambda(y)\leqslant t}\mathrm{d}y_1\cdots\mathrm{d}y_n=2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}t^n/n!.$$

根据引理 3, 对于 K 中非零整理想 $\mathfrak{a}$, $\sigma(\mathfrak{a})$ 为 $\mathbb{R}^n$ 中的格, 并且

$$V(\sigma(\mathfrak{a}))=2^{-r_2}N(\mathfrak{a})|d(K)|^{1/2}.$$

当 $t^n=\left(\frac{4}{\pi}\right)^{r_2}N(\mathfrak{a})|d(K)|^{1/2}n!$ 时, $\mu(B_t)=2^nV(\sigma(\mathfrak{a}))$. 从而由 Minkowski 定理可知存在 $0\neq x\in\mathfrak{a}$, 使得 $\sigma(x)\in B_t$, 即 $\lambda(\sigma(x))\leqslant t$. 于是

$$
\begin{aligned}
|N_{K/\mathbb{Q}}(x)| &= \prod_{i=1}^{n}|\sigma_i(x)|\leqslant\left(\frac{1}{n}\sum_{i=1}^{n}|\sigma_i(x)|\right)^n=\frac{1}{n^n}(\lambda(\sigma(x)))^n \\
&\leqslant\frac{1}{n^n}t^n=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}N(\mathfrak{a}).
\end{aligned}
$$

(b) 设 $\mathfrak{a}'\in C$. 由于 $\mathfrak{a}'$ 除以任何整数之后仍为理想类 C 中的理想,因此可以不妨设 $\mathfrak{a}=\mathfrak{a}'^{-1}$ 是整理想. 由(a)知道有 $0\neq x\in\mathfrak{a}$, $N(x)\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}N(\mathfrak{a})$. 令 $\mathfrak{B}=x\mathfrak{a}^{-1}=x\mathfrak{a}'$. 由于 $x\in\mathfrak{a}$ 可知 $\mathfrak{B}$ 为 C 中整理想,并且

$$N(\mathfrak{B})=N(x)N(\mathfrak{a}')\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}N(\mathfrak{a}\mathfrak{a}').$$

由于 $N(\mathfrak{a}\mathfrak{a}')=N(O_k)=1$,于是证毕. ▮

引理 5 当 $n=[K:\mathbb{Q}]\geqslant 2$ 时, $|d(K)|\geqslant\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. 从而有绝对常数 N,使得对每个数域 K 均有 $n/\log|d(K)|\leqslant N$.

证明 由于数域 K 的每个非零整理想的范均$\geqslant 1$, 所以由引理 4, (b) 即知 $|d(K)|^{1/2}\geqslant\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}$. 于是

$$|d(K)|\geqslant\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{n^n}{n!}\right)^2\geqslant\left(\frac{\pi}{4}\right)^n\left(\frac{n^n}{n!}\right)^2.$$

然后对 n 用归纳法不难证明上式右边 $\geqslant\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$, 从而得到引理 5 的第一论断, 然后立即得到第二论断. ▮

有了上面的准备,我们很容易得到下面一些重要结果.

定理 2 (Minkowski) 对于每个数域 $K\neq\mathbb{Q}$,均有 $|d(K)|>1$. 从而至少一个素数在 K 中分歧.

证明 由于 $n=[K:\mathbb{Q}]\geqslant 2$,根据引理 5 可知

$$|d(K)|\geqslant\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}>1.$$

再由 Dedekind 判别式定理便知至少有一个素数在 K 中分歧. ▮

定理 3 (Dirichlet 类数有限性定理) 每个数域 K 的理想类数 $h(K)=|C(K)|$ 均有限.

证明 对于每个 $q\in\mathbb{Z}$, $q\geqslant 1$,我们有

$$N(\mathfrak{a})=q\Rightarrow|O_K/\mathfrak{a}|=q\Rightarrow\bar{q}=\bar{0}\in O_K/\mathfrak{a}\Rightarrow\mathfrak{a}\,|\,qO_K.$$

由 qO_K 的素理想分解式可知 qO_K 只有有限个整理想因子,从而也只有有限多整理想 $\mathfrak{a}$ 使得 $N(\mathfrak{a})=q$. 从而

$$N(\mathfrak{b}) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{1/2}$$

的整理想 $\mathfrak{b}$ 也只有有限多个. 根据引理 4(b), K 的每个理想类中均包含有这样的整理想 $\mathfrak{b}$, 这就表明 K 只有有限多个理想类. ∎

定理 4 (Hermit) 对于每个固定的 $d \in \mathbb{Z}$, 只有有限多个数域 K 使得 $d(K)=d$.

证明 设 $d(K)=d$. 由 $n \leqslant M \cdot \log|d|$ (引理 5) 可知 K 的次数有界, 从而满足 $r_1+2r_2=n$ 的 n, r_1, r_2 也只有有限多个可能, 因此只需对固定的一组 n, r_1, r_2 证明定理即可.

当 $r_1>0$ 时, 令

$$B=\left\{(y_1, \cdots, y_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{l} |y_1| \leqslant 2^{n-1}\left(\frac{\pi}{2}\right)^{-r_2}|d|^{1/2}, \\ |y_i| \leqslant 1/2 \quad (2 \leqslant i \leqslant r_1), \\ (y_{r_1+j}^2+y_{r_1+r_2+j}^2)^{1/2} \leqslant 1/2 \\ \qquad (1 \leqslant j \leqslant r_2). \end{array}\right\}$$

而当 $r_1=0$ 时, 令

$$B=\left\{(y_1, \cdots, y_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{l} |2y_1| \leqslant 1/2, \ |2y_{r_2+1}| \\ \qquad \leqslant 2^n\left(\frac{\pi}{2}\right)^{1-r_2}|d|^{1/2}; \\ (y_j^2+y_{r_2+j}^2)^{1/2} \leqslant 1/2 \\ \qquad (2 \leqslant j \leqslant r_2). \end{array}\right\}.$$

易知 B 为 $\mathbb{R}^n$ 中关于原点对称的紧凸集. 当 $r_1>0$时,

$$\mu(B)=2^n\left(\frac{\pi}{2}\right)^{-r_2}|d|^{1/2}\left(\frac{\pi}{4}\right)^{r_2}=2^{n-r_2}|d|^{1/2}.$$

而当 $r_1=0$ 时, 也有

$$\mu(B)=\frac{1}{2} \cdot \left(\frac{\pi}{2}\right)^{1-r_2} \cdot 2^n \cdot |d|^{1/2}\left(\frac{\pi}{4}\right)^{r_2-1}=2^{n-r_2}|d|^{1/2}.$$

而 $V(\sigma(O_K))=2^{-r_2}|d|^{1/2}$. 根据引理 2 可知存在 $0 \neq x \in O_K$, 使得 $\sigma(x) \in B$. 我们来证明 $K=\mathbb{Q}(x)$:

当 $r_1>0$ 时, 由于 $i \neq 1$ 时 $|\sigma_i(x)| \leqslant 1/2$, 而

$$|N(x)|=\prod_{i=1}^{n}|\sigma_i(x)| \geqslant 1,$$

因此$|\sigma_1(x)|\geqslant 1$，于是$\sigma_1(x)\neq\sigma_i(x)\ (2\leqslant i\leqslant n)$，从而$\sigma_i(x)\ (1\leqslant i\leqslant n)$彼此不同. 对于$r_1=0$的情形同样可证

$$|\sigma_1(x)|=|\overline{\sigma_1(x)}|\geqslant 1,\quad |\sigma_j(x)|=|\overline{\sigma_j(x)}|\leqslant 1/2\ (2\leqslant j\leqslant r_2).$$

由$|\mathrm{Re}(\sigma_1(x))|\leqslant 1/4$，$|\sigma_1(x)|\geqslant 1$可知$\mathrm{Im}(\sigma_1(x))\neq 0$. 因此

$$\sigma_1(x)\neq\overline{\sigma_1(x)},$$

当$\sigma_j\neq\sigma_1$和$\bar{\sigma}_1$时，$|\sigma_j(x)|\leqslant 1/2$，从而$\sigma_1(x)\neq\sigma_j(x)$. 于是$\sigma_j(x)\ (1\leqslant j\leqslant n)$也两两不同. 因此，在任何情形下，$x$均有$n$个不同的共轭元素. 从而$x$的极小多项式的次数$\geqslant n$，于是$[\mathbb{Q}(x):\mathbb{Q}]\geqslant n$. 但是$\mathbb{Q}(x)\subseteq K$，从而$[\mathbb{Q}(x):\mathbb{Q}]\leqslant[K:\mathbb{Q}]=n$. 所以$[\mathbb{Q}(x):\mathbb{Q}]=n$，即$\mathbb{Q}(x)=K$.

由于$x\in B$，从B的定义可知$|\sigma_i(x)|\ (1\leqslant i\leqslant n)$均有一个只依赖于$n$, d, r_1, r_2的上界. 而x的极小多项式的系数为$\sigma_i(x)\ (1\leqslant i\leqslant n)$的初等对称函数. 所以这些系数的绝对值也有只依赖于n, d, r_1, r_2的上界. 但是这些系数为有理整数，从而只有有限多这样的极小多项式，于是也只有有限多这样的元素x和有限多个数域$K=\mathbb{Q}(x)$. 这就证明了定理. ▮

定理3的证明事实上给出了计算数域类群和类数的一个方法，这就是：首先计算数域K的Minkowski常数

$$M(K)=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d(K)|^{1/2}.$$

根据定理3，每个理想类均有整理想$\mathfrak{B}$，使得$N(\mathfrak{B})\leqslant M(K)$. 因此，如果我们对每个有理素数$p\leqslant M(K)$，将$pO_K$作素理想分解，即求出$p$的全部素理想因子$\mathfrak{p}$，不难看出，类群$C(K)$是由集合$A=\{[\mathfrak{p}]\,|\,\mathfrak{p}|p\leqslant M(K)\}$生成的，其中$[\mathfrak{p}]$表示素理想$\mathfrak{p}$所在的理想类. 当集合$A$不太大时，考查$A$中诸元素之间的乘法关系，就可决定类群$C(K)$和类数$h(K)$. 下面我们举一些例子.

例1 实二次域$K=\mathbb{Q}(\sqrt{d})$，$d>0$，无平方因子，$n=2$，$r_2=0$，从而$M(K)=\dfrac{1}{2}|d(K)|^{1/2}$.

对于$K=\mathbb{Q}(\sqrt{5})$，$d(K)=5$，$M(K)<2$. 于是域K的每

个理想类均有整理想 $\mathfrak{B}$, $N(\mathfrak{B})=1$, 即 $\mathfrak{B}=O_K$. 从而每个理想类均是主理想类. 从而类群 $C(K)=\{1\}$, 类数 $h(K)=1$, 即

$$O_K=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{5})\right]$$

为主理想整环.

对于 $K=\mathbb{Q}(\sqrt{10})$, $d(K)=40$, $M(K)=\frac{1}{2}\sqrt{40}<4$. 素数 2 和 3 在 K 中分解成

$2O_K=\mathfrak{p}^2$, $N(\mathfrak{p})=2$, $\mathfrak{p}=(\sqrt{10},2)$ 不为主理想, $[\mathfrak{p}]^2=1$.

$3O_K=\mathfrak{p}_1\mathfrak{p}_2$, $N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=3$, $\mathfrak{p}_1=(1+\sqrt{10},3)$,

$\mathfrak{p}_2=(1-\sqrt{10},3)$, 均不为主理想, $[\mathfrak{p}_1]=[\mathfrak{p}_2]^{-1}$

(由于 $[\mathfrak{p}_1\mathfrak{p}_2]=[3O_K]=1$),

于是 $C(K)$ 由 $\{[\mathfrak{p}],[\mathfrak{p}_1]\}$ 生成. 由于

$$\begin{aligned}\mathfrak{p}\mathfrak{p}_1&=(\sqrt{10},2)(1+\sqrt{10},3)\\&=(10+\sqrt{10},2+2\sqrt{10},3\sqrt{10},6)\supseteq(2-\sqrt{10})\end{aligned}$$

(因为 $10+\sqrt{10}-(2+2\sqrt{10})-6)=2-\sqrt{10}$). 从而

$$\mathfrak{a}\mathfrak{p}\mathfrak{p}_1=(2-\sqrt{10}),$$

$\mathfrak{a}$ 是某个整理想. 取范得到 $N(\mathfrak{a})\cdot2\cdot3=|N(2-\sqrt{10})|=6$. 于是 $N(\mathfrak{a})=1$, 即 $\mathfrak{a}=O_K$, 从而 $\mathfrak{p}\mathfrak{p}_1$ 为主理想 $(2-\sqrt{10})$. 这就表明 $[\mathfrak{p}]=[\mathfrak{p}_1]^{-1}$. 于是 $C(K)$ 是由 $[\mathfrak{p}]$ 生成的 2 阶群, 而 $h(K)=2$.

例 2 虚二次域 $K=\mathbb{Q}(\sqrt{-d})$, $d>0$, 无平方因子, $n=2$, $r_2=1$, 从而 $M(K)=\frac{2}{\pi}|d(K)|^{1/2}$.

对于 $K=\mathbb{Q}(\sqrt{-23})$, $M(K)=\frac{2}{\pi}\sqrt{23}<4$. 由 $-23\equiv1 \pmod 8$ 可知 2 在 K 中完全分裂:

$$2O_K=\mathfrak{p}_1\mathfrak{p}_2,\ [\mathfrak{p}_1]=[\mathfrak{p}_2]^{-1},\ N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=2.$$

注意 $O_K=\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-23}}{2}\right)$. 如果 $\mathfrak{p}_1$ 为主理想, 则

$$\mathfrak{p}_1=\left(a+\frac{1+\sqrt{-23}}{2}b\right),$$

从而
$$2=N(\mathfrak{p}_1)=\left(a+\frac{b}{2}\right)^2+\frac{23}{4}b^2,$$
于是$(2a+b)^2+23b^2=8$. 但是易知此不定方程无解 $a, b\in\mathbb{Z}$. 这就表明 $\mathfrak{p}_1$ 不为主理想, 即$[\mathfrak{p}_1]\neq 1$. 类似地, 由$\left(\frac{-23}{3}\right)=1$ 可知 3 在 K 中也完全分裂: $3O_K=\mathfrak{q}_1\mathfrak{q}_2$, $[\mathfrak{q}_1]=[\mathfrak{q}_2]^{-1}$, $N(\mathfrak{q}_1)=N(\mathfrak{q}_2)=3$. 由于不定方程$(2a+b)^2+23b^2=12$ 也无有理整数解 $a, b\in\mathbb{Z}$, 因此$[\mathfrak{q}_1]\neq 1$, 进而, $(2a+b)^2+23b^2=24$ 有解$(a, b)=(0, 1)$, 因此若令 $\mathfrak{a}=\left(\frac{1+\sqrt{-23}}{2}\right)$, 则 $N(\mathfrak{a})=6$, 于是 $\mathfrak{a}$ 为某个 $\mathfrak{p}_i$ 乘以某个 $\mathfrak{q}_j$, 即某个$[\mathfrak{p}_i]$和某个$[\mathfrak{q}_j]$相乘为 1. 这就表明 $C(K)$ 是由一元$[\mathfrak{p}_1]$生成的循环群. 由于$(2a+b)^2+23b^2=16$ 无有理整数解, 从而$[\mathfrak{p}]^2\neq 1$. 但是$(2a+b)^2+23b^2=32$ 有解$(a, b)=(1, 1)$. 即对于主理想 $\mathfrak{a}=\left(1+\frac{1+\sqrt{-23}}{2}\right)$, $N(\mathfrak{a})=8$, 从而 $\mathfrak{a}=\mathfrak{p}_1^3, \mathfrak{p}_1^2\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2^2$ 或 $\mathfrak{p}_2^3$. 于是 $1=[\mathfrak{p}_1]^3$, $[\mathfrak{p}_1]^2[\mathfrak{p}_2]$, $[\mathfrak{p}_1][\mathfrak{p}_2]^2$ 或$[\mathfrak{p}_2]^3$. 如果$[\mathfrak{p}_1]^2[\mathfrak{p}_2]=1$, 由于$[\mathfrak{p}_1]=[\mathfrak{p}_2]^{-1}$得到$[\mathfrak{p}_1]=1$, 这是不对的. 因此$[\mathfrak{p}_1]^2[\mathfrak{p}_2]\neq 1$, 同样地$[\mathfrak{q}_1][\mathfrak{q}_2]^2\neq 1$. 于是只能是$[\mathfrak{q}_1]^3$ 或$[\mathfrak{q}_2]^3=1$, 这均表明$[\mathfrak{q}_1]$为三阶元素. 于是 $C(K)$ 是由 $[\mathfrak{q}_1]$生成的 3 阶循环群, 而类数 $h(K)=3$.

对于 $K=\mathbb{Q}(\sqrt{-67})$, $M(K)=\frac{2}{\pi}\sqrt{67}<6$. 由
$$-67\equiv 5\pmod 8),\left(\frac{-67}{3}\right)=\left(\frac{-67}{5}\right)=-1,$$
可知 2, 3, 5 在 K 中均是惯性的. 这就表明 $N(\mathfrak{a})\leqslant 5$ 的整理想$\mathfrak{a}$均是主理想. 从而 $C(K)$ 只包括主理想类, 即 $h(K)=1$. 类似方法可证得对于 $K=\mathbb{Q}(\sqrt{-d})$, $d=1, 2, 3, 7, 11, 19, 43, 67$ 和 163, 均有 $h(K)=1$(习题 4). 高斯曾经猜想: 虚二次域当中只有这九个域的类数为 1. 这个猜想直到 1967 年才由英国数学家 Baker 和美国数学家 Stark 分别独立地证明. 高斯关于二次域类数问题的另一个著名猜想是: 存在着无穷多个实二次域其类数为 1. 这个猜想直到现在既未被证明亦未被推翻. 我们在本书第 II

部分要指明证明这一猜想的困难所在。

例 3 $K=\mathbb{Q}(\omega)$，$\omega^3-2\omega+2=0$。这是对 2 的 Eisenstein 型数域。从我们已经讲过的 Eisenstein 型数域一般结果可知 $2\nmid|O_K/\mathbb{Z}[\omega]|$，而 $d_K(1, \omega, \omega^2)=-(4\cdot(-2)^3+27\cdot 2^2)=-4\cdot 19$。于是 $d(K)=-4\cdot 19$ 并且 $O_K=\mathbb{Z}[\omega]$。由 $d(K)<0$ 知 x^3-2x+2 只有一个实根，于是 $n=3$，$r_1=r_2=1$。所以

$$M(K)=\left(\frac{4}{\pi}\right)\cdot\frac{6}{3^3}\cdot 2\sqrt{19}=2.4\cdots.$$

因为 K 是对 2 的 Eisenstein 型数域，从而 $2O_K=\mathfrak{p}^3$。即只有 $\mathfrak{p}$ 是 $N(\mathfrak{q})=2$ 的整理想。因为 K 的每个理想类必然包含 O_K 或者 $\mathfrak{p}$，从而 $h(K)\leqslant 2$。并且 $h(K)$ 为元素 $[\mathfrak{p}]$ 的阶。但是由 $\mathfrak{p}^3=2O_K$ 知 $[\mathfrak{p}]^3=1$，而 $[\mathfrak{p}]$ 不可能为 3 阶元素（因为 $h(K)\leqslant 2$），从而只可能 $[\mathfrak{p}]=1$，于是 $h(K)=1$。

但是当 $M(K)$ 很大的时候，上述方法计算起来是相当麻烦的。我们在本书第 II 部分将要引进更有效的解析工具来研究数域的类数。

习　　题

1. 设 $\mathfrak{a}$ 为 n 次数域 K 中的分式理想，$\sigma: K\to\mathbb{R}^n$ 为正则嵌入，则 $\sigma(\mathfrak{a})$ 为 $\mathbb{R}^n$ 中的格，并且 $V(\sigma(\mathfrak{a}))=2^{-r_2}N(\mathfrak{a})|d(K)|^{1/2}$。
2. 设 $a, b, c\in\mathbb{R}$，$4ac-b^2>0$。求证当 $f\geqslant\frac{2}{\pi}\sqrt{4ac-b^2}$ 时，存在 $(x, y)\in\mathbb{Z}^2$，$(x, y)\neq(0, 0)$，使得 $ax^2+bxy+cy^2\leqslant f$。
3. (a) 求以下实二次域的类群和类数：
$$K=\mathbb{Q}(\sqrt{d}),$$
$$d=2, 3, 5, 6, 7, 11, 13, 14, 15, 17, 19, 21, 22, 23;$$
   (b) 求以下虚二次域的类群和类数：
$$K=\mathbb{Q}(\sqrt{-d}),$$
$$d=1, 2, 3, 5, 6, 7, 10, 11, 13, 15, 17, 19, 23, 43, 163;$$
   (c) 求数域 $K=\mathbb{Q}(\omega)$，$\omega^3+\omega+1=0$ 的理想类数。
4. 设 $K=\mathbb{Q}(\sqrt{-d})$，$d>0$，无平方因子，并且 $h(K)=1$。求证：

(a) 当 $d \geqslant 10$ 时，必然 $d \equiv 5 \pmod 8$；

(b) 如果 p 为奇素数并且 $d < 4p$，则 $\left(\frac{d}{p}\right) = -1$；

(c) 如果 $d > 19$，则 $d \equiv -43, -67, -163, -403, -547$ 或者 -667 $(\bmod 840)$；

(d) 如果 $d > 163$，则必然 $d > 2000$.

5. 求证：

(a) $K = \mathbb{Q}(\sqrt{-14})$ 的类群是 4 阶循环群；

(b) $K = \mathbb{Q}(\sqrt{-21})$ 的类群是两个 2 阶循环群的直积；

(c) $K = \mathbb{Q}(\sqrt{-103})$ 的类数是 5.

6. 求证：

(a) $\mathbb{Q}(\omega)$ 和 $\mathbb{Q}(\omega + \omega^{-1})$ $(\omega = \zeta_7)$ 的类数均是 1；

(b) $\mathbb{Q}(\omega + \omega^{-1})$ $(\omega = \zeta_{11})$ 的类数是 1.

7. 求证：

(a) $\mathbb{Z}[\sqrt[3]{2}]$ 和 $\mathbb{Z}[\alpha]$ $(\alpha^3 = \alpha + 1,\ \alpha \in \mathbb{R})$ 均是主理想整环；

(b) $\mathbb{Z}[\sqrt[3]{m}]$ $(m = 3, 5, 6)$ 均是主理想整环；

(c) $\mathbb{Z}[\omega]$ $(\omega \in \mathbb{R},\ \omega^3 = \omega - 1)$ 是主理想整环.

§2 Dirichlet 单位定理

2.1 Dirichlet 单位定理

对于每个数域 K，我们以 U_K 表示整数环 O_K 的单位群，即 U_K 是 O_K 中乘法可逆元素全体所形成的乘法群. 本节的主要目的是决定单位群 U_K 的结构. 我们在第一章已经知道，数域 K 中的单位根（即乘法有限阶元素）全体是有限循环群，表示成 W_K，这是乘法 Abel 群 U_K 的扭子群. 根据附录 B(1) 可知，U_K 中存在一个无扭子群（即自由 Abel 群）V_K，使得 $U_K = W_K \times V_K$（直积）. 我们要证明，自由 Abel 群 V_K 的秩是有限的，并且等于 $r_1 + r_2 - 1$，其中 r_1 和 r_2 分别是 K 到 $\mathbb{C}$ 中的实嵌入个数和复嵌入对数. 这就是著名的 Dirichlet 单位定理. 在证明此定理之前，首先给出 O_K 中元素属于 U_K 或者 W_K 的判别条件.

引理 6 设 K 为 n 次数域，$\sigma_1, \cdots, \sigma_n$ 是 K 到 $\mathbb{C}$ 中的 n 个嵌入，$u \in O_K$. 则

(a) $u\in U_K \Leftrightarrow N_{K/\mathbb{Q}}(u)=\pm 1$;

(b) $u\in W_K \Leftrightarrow |\sigma_i(u)|=1 (1\leqslant i\leqslant n)$.

证明 (a) 如果 $u\in U_K$，则 $u^{-1}\in O_K$. 于是 $N(u)$, $N(u^{-1})\in \mathbb{Z}$. 但是 $N(u)\cdot N(u^{-1})=N(1)=1$. 从而 $N(u)=\pm 1$. 反之，若 $u\in O_K$, $N(u)=\pm 1$，则 u 是多项式

$$f(x)=\sum_{i=1}^{n}(x-\sigma_i(u))=x^n+a_{n-1}x^{n-1}+\cdots+a_1x\pm 1\in \mathbb{Z}[x]$$

的根. 于是 u^{-1} 为 $\mathbb{Z}[x]$ 中首1多项式 $x^n\pm(a_1x^{n-1}+\cdots+a_{n-1}x+1)$ 的根，从而 $u^{-1}\in O_K$，即 $u\in U_K$.

(b) 如果 u 为单位根，即存在某个 $m\in\mathbb{Z}$，使得 $u^m=1$，则

$$\sigma_i(u)^m=\sigma_i(u^m)=1 (1\leqslant i\leqslant n).$$

于是 $|\sigma_i(u)|=1 (1\leqslant i\leqslant n)$. 反之，设 $u\in O_K$, $|\sigma_i(u)|=1 (1\leqslant i\leqslant n)$，则 $u^j (j\in\mathbb{Z})$ 是 n 次多项式

$$f(x)=\prod_{i=1}^{n}(x-\sigma_i(u^j))=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$$

的根. a_i 均是 $\sigma_1(u^j)$, $\cdots$, $\sigma_n(u^j)$ 的初等对称函数，但是

$$|\sigma_1(u^j)|=\cdots=|\sigma_n(u^j)|=1,$$

因此 $|a_i|\leqslant \binom{n}{i} (0\leqslant i\leqslant n-1)$. $\mathbb{Z}[x]$ 中这样的多项式只有有限多个，从而存在两个有理整数 j, k, $j>k$，使得 $u^j=u^k$. 由于 $u\neq 0$，从而 $u^{j-k}=1$. 这就表明 u 是单位根. ∎

定理 5 (Dirichlet 单位定理) 设 K 为 n 次数域，K 到 $\mathbb{C}$ 中有 r_1 个实嵌入和 r_2 对复嵌入，$r_1+2r_2=n$，则 $U_K=W_K\times V_K$（直积），其中 W_K 是 K 中单位根群（有限循环群），而 V_K 是秩为 $r=r_1+r_2-1$ 的自由 Abel 群.

证明 考虑对数映射

$$l: U_K\to \mathbb{R}^{r_1+r_2},\ l(\eta)=(\lambda_1\log|\eta^{(1)}|, \cdots, \lambda_{r_1+r_2}\log|\eta^{(r_1+r_2)}|),$$

其中 $\eta^{(i)}=\sigma_i(\eta)$, $\lambda_i=1$（对于 $1\leqslant i\leqslant r_1$），2（对于 $r_1+1\leqslant i\leqslant r_1+r_2$）. 易知 l 是从乘法群 U_K 到加法群 $\mathbb{R}^{r_1+r_2}$ 中的同态. 根据引理 6(b) 可知

$$\eta\in\operatorname{Ker} l \Leftrightarrow \log|\eta^{(i)}|=0 (1\leqslant i\leqslant r_1+r_2)$$

$$\Leftrightarrow |\eta^{(i)}|=1(1\leqslant i\leqslant n)\Leftrightarrow \eta\in W_K,$$

因此 $\mathrm{Ker}\, l=W_K$. 于是 $V_K=U_K/W_K\cong l(U_K)$. 另一方面，如果 $\eta\in U_K$，则由引理 6(a)知

$$\sum_{i=1}^{r_1+r_2}\lambda_i\log|\eta^{(i)}|=\sum_{i=1}^{n}\log|\eta^{(i)}|=\log|N(\eta)|=0.$$

这就表明象集合 $l(U_K)$ 是 $\mathbb{R}^{r_1+r_2}$ 的超平面

$$H=\{(a_1,\ \cdots,\ a_{r_1+r_2})\in\mathbb{R}^{r_1+r_2}|a_1+\cdots+a_{r_1+r_2}=0\}$$

的一个加法子群. 进而，对于 $\mathbb{R}^{r_1+r_2}$ 的每个有界子集 B，则存在一个常数 M，使得 $(a_1,\ \cdots,\ a_{r_1+r_2})\in B$ 时，$|a_i|\leqslant M(1\leqslant i\leqslant r_1+r_2)$. 于是若 $l(\eta)\in B$，则 $|\eta^{(i)}|\leqslant e^M(1\leqslant i\leqslant n)$. 从而 η 所满足的多项式

$$\prod_{i=1}^{n}(x-\eta^{(i)})=x^n+a_1x^{n-1}+\cdots+a_n\in\mathbb{Z}[x]$$

的诸系数也是有界的：$|a_i|\leqslant e^M\cdot\binom{n}{i}$. 这样的多项式只有有限多个，从而满足 $l(\eta)\in B$ 的元素 $\eta\in U_K$ 也只有有限多个，即 $l(U_K)\cap B$ 是有限集合. 这就表明 $l(U_K)$ 是 $\mathbb{R}^{r_1+r_2}$ 的离散子群. 根据§6中引理 2，$l(U_K)$ 是 $\mathbb{R}^{r_1+r_2}$ 的某个子空间中的格. 由于 $l(U_K)\subseteq H$，可知 $l(U_K)$ 的秩 $\leqslant r_1+r_2-1$. 为了完成定理 5 的证明，我们只需再证 $l(U_K)$ 中存在 r 个 $\mathbb{Z}$-线性无关元素即可. 这需要以下三个引理：

引理 7 对于 $0\neq\alpha\in O_K$，我们也定义

$$l(\alpha)=(a_1,\ \cdots,\ a_{r_1+r_2})=(\lambda_1\log|\alpha^{(1)}|,\ \cdots,\ \lambda_{r_1+r_2}\log|\alpha^{(r_1+r_2)}|).$$

则对于每个 $0\neq\alpha\in O_K$ 和每个 k，$1\leqslant k\leqslant r_1+r_2$，均存在 $0\neq\beta\in O_K$，使得 $l(\beta)=(b_1,\ \cdots,\ b_{r_1+r_2})$ 满足 $b_i<a_i$（当 $i\neq k$ 时），并且

$$|N(\beta)|\leqslant\left(\frac{2}{\pi}\right)^{r_2}|d(K)|^{1/2}.$$

证明 不妨取 $k=1$. 定义

$$B=\{(x_1,\ \cdots,\ x_n)\in\mathbb{R}^n|\,|x_i|\leqslant c_i(1\leqslant i\leqslant r_1),$$
$$x_j^2+x_{j+r_2}^2\leqslant c_j(r_1+1\leqslant j\leqslant r_1+r_2)\},$$

其中
$$c_1=(c_2\cdots c_{r_1+r_2})^{-1}\left(\frac{2}{\pi}\right)^{r_2}|d(K)|^{1/2},$$

而 $0<c_i<e^{a_i}(2\leqslant i\leqslant r_1+r_2)$. 则

$$\mu(B)=2^{r_1}c_1\cdots c_{r_1}\cdot\pi^{r_2}c_{r_1+1}\cdots c_{r_1+r_2}=2^n\cdot 2^{-r_1}|d(K)|^{1/2}.$$

于是由 Minkowski 定理, 可知有 $0\neq\beta\in O_K$, 使得

$$\lambda_i\log|\beta^{(i)}|\leqslant\log c_i<a_i(2\leqslant i\leqslant r_1+r_2)$$

而
$$|N(\beta)|\leqslant c_1\cdots c_{r_1+r_2}=\left(\frac{2}{\pi}\right)^{r_2}|d(K)|^{1/2},$$

从而 β 即为所求. ▌

引理 8 对每个 $k(1\leqslant k\leqslant r_1+r_2)$, 均有

$$u_k\in U_K,\ l(u_k)=(y_1,\ \cdots,\ y_{r_1+r_2}),$$

使得当 $i\neq k$ 时, $y_i<0$.

证明 从任意一个 $\alpha_1\in O_K-\{0\}$开始, 根据引理 7 依次求出 $\alpha_2,\ \alpha_3,\ \cdots,\ \in O_K-\{0\}$, 使得当 $i\neq k$ 时均有 $(l(\alpha_{j+1}))_i<(l(\alpha_j))_i$ (这里 $(l(\alpha))_i$ 表示向量 $l(\alpha)\in\mathbb{R}^{r_1+r_2}$ 的第 i 个坐标), 并且 $|N(\alpha_j)|\leqslant M$. 由最后一个条件可知主理想集合 $\{\alpha_jO_K|j=1,\ 2,\cdots\}$ 是有限集合. 从而有 $j>h$, 使得 $\alpha_jO_K=\alpha_hO_K$. 令 $\alpha_j=u_k\alpha_h$, 则 $u_k\in U_K$, 并且满足引理条件. ▌

利用引理 8, 我们得到 r_1+r_2 个单位 u_k, 使得

$$l(u_k)=(y_{k1},\ \cdots,\ y_{k,r_1+r_2}),$$

而 r_1+r_2 阶实方阵 (y_{ij}) 的元素符号有形式

$$((\mathrm{sgn}\,y_{ij}))=\begin{pmatrix}+ & & -\\ & + & \\ - & & \ddots & \\ & & & +\end{pmatrix},$$

并且 (y_{ij}) 的每行之和均为零. 为证 $l(u_k)\ (1\leqslant k\leqslant r_1+r_2)$ 中有

$$r=r_1+r_2-1$$

个线性无关, 我们只需证明方阵 (y_{ij}) 的秩为 r 即可, 而这可由下面的一般性引理推出.

引理 9 设 $A=(a_{ij})$ 为 m 阶实方阵, 主对角线上元素为正, 而其余元素均为负, 并且每行元素之和均为 0, 则

$$\mathrm{rank}\,A=m-1.$$

证明 设$(a_{ij})=(v_1, \cdots, v_m)$, v_i为列向量$\begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}$,如果其中有$m-1$个列向量是线性相关的. 必要时对于方阵$A$的诸行和诸列作一个适当的置换,不妨设$A$的前$m-1$列线性相关. 则有不全为0的$t_i\in\mathbb{R}$,使得$\sum_{i=1}^{m-1}t_iv_i=0$(零列向量). 必要时乘以适当常数之后,可设$t_k=1$,而其余$|t_j|\leqslant 1 (1\leqslant j\leqslant m-1, j\neq k)$. 现在考虑$A$的第$k$行,便有

$$0=\sum_{j=1}^{m}a_{kj}<\sum_{j=1}^{m-1}a_{kj}\leqslant\sum_{j=1}^{m-1}t_ja_{kj}=0$$

这就导致矛盾. 因此$\operatorname{rank} A=m-1$. ▌

这就完全证明了定理5. 这个定理也可叙述成如下形式: 数域K中存在着$r=r_1+r_2-1$个单位$\eta_1, \cdots, \eta_r\in U_K$,使得每个单位$\eta\in U_K$均可唯一地表示成

$$\eta=w\eta_1^{a_1}\cdots\eta_r^{a_r},\ w\in W_K,\ a_i\in\mathbb{Z}.$$

这样一组单位$\{\eta_1, \cdots, \eta_r\}$称作是域$K$的一个基本单位组. 如果$\{\varepsilon_1, \cdots, \varepsilon_r\}$又是$K$的一个基本单位组,则易知

$$\varepsilon_i=w_i\sum_{j=1}^{r}\eta_j^{a_{ij}},\ w_i\in W_K,\ a_{ij}\in\mathbb{Z},\ \det(a_{ij})=\pm1.$$

以外,如果令$l(\eta_i)=(y_{i1}, \cdots, y_{i,r+1})$ (l为对数映射),并且定义

$$R(\eta_1, \cdots, \eta_r)=|\det(y_{ij})_{1\leqslant i,j\leqslant r}|.$$

则(由于$\log|\varepsilon_k^{(i)}|=\sum_{j=1}^{r}a_{kj}\log|\eta_j^{(i)}|$)

$$\begin{aligned} R(\varepsilon_1, \cdots, \varepsilon_r) &= |\det(\lambda_i\log|\varepsilon_k^{(i)}|)_{1\leqslant i,k\leqslant r}| \\ &=2^{\max(r_2-1,0)}|\det(\log|\varepsilon_k^{(i)}|)| \\ &=2^{\max(r_2-1,0)}|\det(\log|\eta_k^{(i)}|)|\cdot|\det(a_{ij})| \\ &=R(\eta_1, \cdots, \eta_r). \end{aligned}$$

这就表明实数$R(\eta_1, \cdots, \eta_r)$与基本单位组$\{\eta_1, \cdots, \eta_r\}$的取法无关,从而它是数域$K$的不变量,我们称它为数域$K$的**regulator**,并且记成$R(K)$. 我们在本书第Ⅱ部分将会看到,$R(K)$混在类

数 $h(K)$ 的解析公式之中. 对于一般的数域 K, 寻求 K 的基本单位组是件相当困难的事情. 因此 $R(K)$ 也是用类数解析公式计算类数 $h(K)$ 的一个主要困难所在.

以下两小节我们举一些计算基本单位组的例子.

2.2 实二次域的基本单位, Pell 方程

对于虚二次域 K, $r_1=0$, $r_2=1$, 于是 $r=r_1+r_2-1=0$, 这表明单位群 U_K 就是单位根群 W_K. 而在第一章中我们已经完全决定了虚二次域的单位根群, 从而也就完全决定了虚二次域的单位群.

现在我们考虑实二次域 $K=\mathbb{Q}(\sqrt{d})$, $d>0$, 无平方因子. 这时 $r_1=2$, $r_2=0$, $r=r_1+r_2-1=1$. 即 K 的基本单位组由一个单位 ε 构成. 称 ε 为实二次域 K 的基本单位. 由于 $W_K=\{\pm 1\}$, 因此 $U_K=\{\pm\varepsilon^n | n\in\mathbb{Z}\}$. 不难看出, 可以作为基本单位的只有 $\pm\varepsilon$ 和 $\pm\varepsilon^{-1}$, 从而满足 $\varepsilon>1$ 的基本单位是唯一确定的.

对于 $d\equiv 2, 3 \pmod 4$ 的情形, $O_K=\mathbb{Z}[\sqrt{d}]$. 从而 K 中整数可写成 $a+b\sqrt{d}$, $a, b\in\mathbb{Z}$. 而 $a+b\sqrt{d}$ 为 K 中单位 $\Leftrightarrow$

$$N(a+b\sqrt{d})=a^2-db^2=\pm 1$$

(引理 6). 二元二次不定方程 $x^2-dy^2=\pm 1$ 称作是 Pell 方程. 于是我们看到, Pell 方程在 $\mathbb{Z}$ 中的解 (x, y) 与实二次域的单位有密切联系, 而由 U_K 的结构不难得到 Pell 方程全部解的结构. 具体说来就是:

引理 10 设 $K=\mathbb{Q}(\sqrt{d})$, $d>0$, 无平方因子, $d\equiv 2, 3 \pmod 4$. 令 $\varepsilon=a+b\sqrt{d}$ $(a, b\in\mathbb{Z})$ 是域 K 的基本单位, $\varepsilon>1$. 又令 $\varepsilon^n=(a+b\sqrt{d})^n=a_n+b_n\sqrt{d}$, $a_n, b_n\in\mathbb{Z}$.

(a) 如果 $N(\varepsilon)=1$, 则 Pell 方程 $x^2-dy^2=-1$ 无有理整数解, 而 $x^2-dy^2=1$ 的全部有理整数解为 $\{(\pm a_n, \pm b_n) | n\in\mathbb{Z}\}$.

(b) 如果 $N(\varepsilon)=-1$, 则 $x^2-dy^2=-1$ 的全部有理整数解为 $\{(\pm a_{2n+1}, \pm b_{2n+1}) | n\in\mathbb{Z}\}$, 而 $x^2-dy^2=1$ 的全部有理整数解为

$$\{(\pm a_{2n}, \pm b_{2n}) | n\in\mathbb{Z}\}.$$

证明 这是由于如果 $N(\varepsilon)=1$，则 $U_K=\{\pm\varepsilon^n|n\in\mathbb{Z}\}$ 中每个单位的范均为 1. 如果 $N(\varepsilon)=-1$，则范为 1 的单位全体形成 U_K 的一个指数为 2 的子群，并且这个群就是 $\{\pm\varepsilon^{2n}|n\in\mathbb{Z}\}$. 将这些翻译成 Pell 方程的语言即得引理. ▌

注记 (1) 对于实二次域 $\mathbb{Q}(\sqrt{d})$，它的基本单位何时范为 1，何时范为 -1? 目前有不少判别法，但是都适用于某些特定的情形(例如习题 7). 对于一般情形目前还没有简便而完整的判别方法.

(2) 我们也可由解 Pell 方程 $x^2-dy^2=\pm1$ 来求实二次域

$$K=\mathbb{Q}(\sqrt{d})\ (d\equiv2,\ 3(\mathrm{mod}\ 4))$$

的基本单位: 设 $a,\ b\in\mathbb{Z}$ 满足 $a^2-db^2=1$ 或 -1, $a+b\sqrt{d}>1$，并且使得 $a+b\sqrt{d}$ 在这些条件下达到最小，称 $(a,\ b)$ 是 Pell 方程 $x^2-dy^2=\pm1$ 的最小解. 显然，对应于这个最小解 $(a,\ b)$，$\varepsilon=a+b\sqrt{d}$ 就是实二次域 $\mathbb{Q}(\sqrt{d})$ 中满足 $\varepsilon>1$ 的基本单位.

设 $(a,\ b)$ 为 Pell 方程 $x^2-dy^2=\pm1$ 的最小解，则必然 $a>0$, $b>0$ (因为 $\pm a\pm b\sqrt{d}$ 中只有一个 >1). 令

$$a_n+b_n\sqrt{d}=(a+b\sqrt{d})^n,\ n=1,\ 2,\ \cdots,$$

则 $$(a+b\sqrt{d})\ (a_{n-1}+b_{n-1}\sqrt{d})=(a_n+b_n\sqrt{d}),$$

于是 $b_n=ab_{n-1}+ba_{n-1}$，从而序列 $\{b_n\}$ 是递增的. 因此，我们可以从 $y=1,\ 2,\ \cdots$ 依次试验 $dy^2\pm1$ 是否为完全平方数. 如果 b 为最小的自然数，使 db^2+1 或 db^2-1 为完全平方数，令 a 为这个完全平方数的正平方根，我们就得到 $x^2-dy^2=\pm1$ 的最小解 $(a,\ b)$，从而也就得到实二次域 $\mathbb{Q}(\sqrt{d})$ 的基本单位 $\varepsilon=a+b\sqrt{d}>1$.

例 $K=\mathbb{Q}(\sqrt{14})$. Pell 方程为 $x^2-14y^2=\pm1$. 由于 14 ± 1, $14\cdot2^2\pm1$ 和 $14\cdot3^2\pm1$ 均不是完全平方数，而 $14\cdot4^2+1=15^2$. 从而 $\varepsilon=15+4\sqrt{14}$ 为 K 的基本单位，而 $N(\varepsilon)=-1$，于是 Pell 方程 $x^2-14y^2=1$ 的全部解为

$$\{(\pm a_{2n},\ \pm b_{2n})\,|\,a_{2n}+b_{2n}\sqrt{14}=(15+4\sqrt{14})^{2n},\ n\in\mathbb{Z}\},$$

而 $x^2-14y^2=-1$ 的全部解为

$$\{(\pm a_{2n+1},\ \pm b_{2n+1})\,|\,a_{2n+1}+b_{2n+1}\sqrt{14}$$

$$=(15+4\sqrt{14})^{2n+1},\ n\in\mathbb{Z}\},$$

对于 $d\equiv1\pmod 4$ 的情形,

$$K=\mathbb{Q}(\sqrt{d}),\ O_K=\mathbb{Z}\oplus\mathbb{Z}\omega,\ \omega=\frac{1}{2}(1+\sqrt{d}).$$

从而 K 中整数表示成

$$a+b\omega=\frac{2a+b}{2}+\frac{b}{2}\sqrt{d}=\frac{A+B\sqrt{d}}{2},\ A,\ B\in\mathbb{Z},$$

$$A\equiv B\pmod 2.$$

而 $\varepsilon=\frac{1}{2}(A+B\sqrt{d})$ 为单位 $\Leftrightarrow A^2-dB^2=\pm4$. 对于这种情形我们有:

引理 11 设 $K=\mathbb{Q}(\sqrt{d}),d>0$, 无平方因子, $d\equiv1\pmod 4$,

$$\varepsilon=\frac{1}{2}(a+b\sqrt{d})>1$$

为域 K 的基本单位, $a,\ b\in\mathbb{Z},\ a\equiv b\pmod 2$. 令

$$\frac{1}{2}(a_n+b_n\sqrt{d})=\varepsilon^n,\ n\in\mathbb{Z},$$

则

(a) 当 $N(\varepsilon)=-1$ 时, $x^2-dy^2=4$ 的全部整解为

$$\{(\pm a_{2n},\ \pm b_{2n})\mid n\in\mathbb{Z}\},$$

而 $x^2-dy^2=-4$ 的全部整解为 $\{(\pm a_{2n+1},\ \pm b_{2n+1})\mid n\in\mathbb{Z}\}$. 当 $N(\varepsilon)=1$ 时, $x^2-dy^2=-4$ 无整解, 而 $x^2-dy^2=4$ 的全部整解为

$$\{(\pm a_n,\ \pm b_n)\mid n\in\mathbb{Z}\}.$$

(b) 当 $N(\varepsilon)=-1$ 时, 如果 $a\equiv b\equiv0\pmod 2$, 则 $x^2-dy^2=-1$ 的全部整解为 $\left\{\left(\pm\frac{1}{2}a_{2n+1},\ \pm\frac{1}{2}b_{2n+1}\right)\middle|\ n\in\mathbb{Z}\right\}$, $x^2-dy^2=1$ 的全部整解为 $\left\{\left(\pm\frac{1}{2}a_{2n},\ \pm\frac{1}{2}b_{2n}\right)\middle|\ n\in\mathbb{Z}\right\}$; 如果 $a\equiv b\equiv1\pmod 2$, 则 $x^2-dy^2=-1$ 的全部整解为 $\left\{\left(\pm\frac{1}{2}a_{6n+3},\ \pm\frac{1}{2}b_{6n+3}\right)\middle|\ n\in\mathbb{Z}\right\}$, $x^2-dy^2=1$ 的全部整解为 $\left\{\left(\pm\frac{1}{2}a_{6n},\ \pm\frac{1}{2}b_{6n}\right)\middle|\ n\in\mathbb{Z}\right\}$. 当 $N(\varepsilon)=1$ 时, $x^2-dy^2=-1$ 无整解. 如果 $a\equiv b\equiv0\pmod 2$, 则 x^2

$-dy^2=1$ 的全部整解为 $\left\{\left(\pm\frac{1}{2}a_n,\ \pm\frac{1}{2}b_n\right)\middle|\, n\in\mathbb{Z}\right\}$，如果 $a\equiv b\equiv1\pmod 2$，则 $x^2-dy^2=1$ 的全部整解为

$$\left\{\left(\pm\frac{1}{2}a_{3n},\ \pm\frac{1}{2}b_{3n}\right)\middle|\, n\in\mathbb{Z}\right\}.$$

证明 对于(a)可象引理10一样地证明．对于(b)，我们只需证明：如果

$$\varepsilon=\frac{1}{2}(a+b\sqrt{d})=\frac{1}{2}(a_1+b_1\sqrt{d})>1,\ a_1\equiv b_1\equiv1\pmod 2),$$

则 $a_2\equiv b_2\equiv1\pmod 2$，而 $a_3\equiv b_3\equiv0\pmod 2$．由此不难得到(b)中全部结果．

设 $\varepsilon=a_1+b_1\sqrt{d}>1,\ a_1\equiv b_1\equiv1\pmod 2$，则

$$a_2+b_2\sqrt{d}=\frac{1}{2}(a_1+b_1\sqrt{d})^2=\frac{1}{2}(a^2+db^2+2ab\sqrt{d}).$$

由于 $a^2\equiv b^2\equiv d\equiv1\pmod 4$，可知

$$a_2=\frac{1}{2}(a^2+db^2)\equiv1\pmod 2,\ b_2=ab\equiv1\pmod 2.$$

另一方面，

$$(a_3+b_3\sqrt{d})=\frac{1}{4}(a_1+b_1\sqrt{d})^3$$

$$=\frac{1}{4}[a^3+3adb^2+(3a^2b+b^3d)\sqrt{d}].$$

由于 $a^2-b^2d=\pm4$，从而

$$a^3+3adb^2=a(a^2+3db^2)=4a(b^2d\pm1)\equiv0\pmod 8,$$

$$3a^2b+b^3d=b(3a^2+b^2d)=4ab(a^2\pm1)\equiv0\pmod 8,$$

从而 $a_3\equiv b_3\equiv0\pmod 2$．这就完全证明了引理11． ▌

注记 对于实二次域 $\mathbb{Q}(\sqrt{d})$，其基本单位 $\varepsilon_d>1$ 究竟有多大？这也是人们长期以来所关心的问题．如果 $d=t^2+4$ 没有平方因子，$t>0$（例如 $t=1,3,5$ 等等），则 $\varepsilon_d=\frac{1}{2}(t+\sqrt{d})$（习题3）．如果 $d=t^2-4$ 无平方因子，$t\geqslant5$，则 $\varepsilon_d=\frac{1}{2}(t+\sqrt{d})$（习题4）．对于这两种情形，$\varepsilon_d$ 差不多等于 $\sqrt{d}$．但是

$$\varepsilon_{67}=48842+5967\sqrt{67},\ \varepsilon_{94}=2143295+221064\sqrt{94},$$

这表明 ε_d 的大小也很没有规律. 关于 ε_d 的目前最好的上界，是由华罗庚于 1942 年得到的.

$$h_K\cdot\log\varepsilon_d<\frac{1}{2}\sqrt{d}\log d+\sqrt{d}.\ (K=\mathbb{Q}(\sqrt{d})),$$

(我们在本书第 II 部分要解释，为什么类数 h_K 和 K 的 regulator $\log\varepsilon_d$ 搅在一起)，特别地有 $\log\varepsilon_d<\frac{1}{2}\sqrt{d}\log d+\sqrt{d}$.

2.3 其他例子

例 1 非全实的实三次域 设 $K=\mathbb{Q}(\alpha)$，α 是实的三次代数数，而 α 的另外两个共轭元素是一对共轭虚数：$\alpha^{(1)}=\alpha\in\mathbb{R}$，$\alpha^{(2)}=a+bi$，$\alpha^{(3)}=a-bi$，$a,\ b\in\mathbb{R}$，$b\neq 0$. 由于 $r_1=r_2=1$，于是 $r=r_1+r_2-1=1$. 从而 K 的基本单位组也只包含一个单位 ε，与实二次域情形一样，我们称 ε 是三次域 K 的基本单位. 并且由于 $W_K=\{\pm 1\}$，从而可以作为基本单位的只能是 $\pm\varepsilon$，$\pm\varepsilon^{-1}$. 于是 $\varepsilon>1$ 的基本单位也是唯一确定的. 而 K 中每个单位均可表示成 $\pm\varepsilon^n$，$n\in\mathbb{Z}$.

引理 12 设 $K=\mathbb{Q}(\alpha)$是实三次域，$r_1=r_2=1$. η 为域 K 的任意一个单位，$\eta>1$. 则

(a) $|d(K)|\leqslant|d_K(1,\ \eta,\ \eta^2)|<4\eta^3+24$;

(b) 如果 α 的极小多项式为 $f(x)=x^3+kx-1$，$k\in\mathbb{Z}$，$k\geqslant 2$ (易知这样的 $f(x)$ 必是 $\mathbb{Q}[x]$ 中不可约多项式)，并且 $4k^3+27$ 无平方因子，则 α^2+k 是域 K 的基本单位.

证明 (a) 由于 $\eta>1$，$\eta\in U_K$，从而 $\eta\notin\mathbb{Q}$. 于是$K=\mathbb{Q}(\eta)$，即 η 与其另外两个共轭元素 $\eta^{(2)}$，$\eta^{(3)}$ 两两不同. 而由假设 $r_1=r_2=1$ 可知 $\eta^{(2)}$ 和 $\eta^{(3)}$ 是一对共轭的复数. 于是 $N(\eta)=\eta\cdot|\eta^{(2)}|^2>0$，即 $N(\eta)=1$. 令 $\eta=u^2(u\in\mathbb{R},\ u>1)$，则 $|\eta^{(2)}|=|\eta^{(3)}|=\frac{1}{u}$，于是 $\eta^{(2)}=\frac{1}{u}e^{iv}$，$\eta^{(3)}=\frac{1}{u}e^{-iv}$，$(0<v<\pi)$. 从而

$$|d_K(1,\ \eta,\ \eta^2)|^{1/2}=\left|\det\begin{pmatrix}1 & \eta & \eta^2\\ 1 & \eta^{(2)} & \eta^{(2)2}\\ 1 & \eta^{(3)} & \eta^{(3)2}\end{pmatrix}\right|$$

$$=\left|\left(u^2-\frac{1}{u}e^{iv}\right)\left(u^2-\frac{1}{u}e^{-iv}\right)\left(\frac{1}{u}e^{iv}-\frac{1}{u}e^{-iv}\right)\right|$$

$$=2(u^3+u^{-3}-2\cos v)\sin v$$

(注意当 $u>1$ 时，$u^3+u^{-3}-2\cos v>2-2=0$，而 $0<v<\pi$ 时 $\sin v>0$) 令 $2t=u^3+u^{-3}$，$x=\cos v$，则

$$|d_K(1,\ \eta,\ \eta^2)|^{1/2}=4(t-x)\sqrt{1-x^2},\quad -1<x<1.$$

固定 u（从而固定 t），将上式右边看作是 x 的函数（$-1<x<1$）：$g(x)=4(t-x)\sqrt{1-x^2}$．当 $-1<x<1$ 时 $g(x)>0$，而 $g(\pm 1)=0$．从而 $g(x)$ 在 $(-1,\ 1)$ 中某点 $x=c$ 有最大值．由于 $g'(x)=4(2x^2-tx-1)/\sqrt{1-x^2}$，从而 $2c^2-tc-1=0$，即 c 为 $h(x)=2x^2-tx-1$ 的根．由于 $h(-1)=1+t>0$，$h(1)=1-t<0$，$h(-u^{-3}/2)=\frac{3}{4}(u^{-6}-1)<0$，从而 $c<-u^{-3}/2$．即 $u^{-6}-4c^2<0$．再由 $tc=2c^2-1$，即 $t^2c^2=4c^4-4c^2+1$，从而

$$|d_K(1,\ \eta,\ \eta^2)|\leqslant 16(t-c)^2(1-c^2)=16(t^2+1-c^2-c^4)$$

$$=4u^6+24+4(u^{-6}-4c^2-4c^4)$$

$$<4u^6+24=4\eta^3+24.$$

最后，$|d(K)|\leqslant|d_K(1,\ \eta,\ \eta^2)|$ 是显然的，因为 $|d_K(1,\eta,\eta^2)|\neq 0$．

(b) 由于 $f(x)$ 的判别式为 $-(4k^3+27)<0$，α 为 $f(x)$ 的实根，从而另外二根为共轭的虚根．于是满足 (a) 中条件，并且 $\alpha\in U_K$．由于 $d(K)|O_K/\mathbb{Z}[\alpha]|^2=d_K(1,\ \alpha,\ \alpha^2)=-(4k^3+27)$，而假定 $4k^3+27$ 无平方因子，从而 $d(K)=-(4k^3+27)$，$O_K=\mathbb{Z}[\alpha]$．设 $\eta>1$ 为 K 中基本单位，则 $|d_K(1,\ \eta,\ \eta^2)|\geqslant|d(K)|=4k^3+27$．但是由 (a) 知 $|d_K(1,\ \eta,\ \eta^2)|\leqslant 4\eta^3+24$，从而 $k<\eta$．如果 $\frac{1}{\alpha}=\alpha^2+k$ 不是基本单位，则由于 α^2+k 是大于 1 的单位，从而 $\alpha^2+k=\eta^t$，$t\geqslant 2$．于是 $k^2<\eta^2\leqslant\eta^t=\alpha^2+k<1+k$．当 $k\geqslant 2$ 时这不可能．因此 α^2+k 必为 K 中基本单位． ▮

例如 $k=2, 4, 5$ 时，$4k^3+27=59$，283，527 均无平方因子．取 ε 为 $x^3+kx-1\,(k=2, 4, 5)$ 的实根，则 ε 为域 $K=\mathbb{Q}(\varepsilon)$ 的基本单位($0<\varepsilon<1$)．可以证明：对于无限多个 $k\geqslant 2$，$4k^3+27$ 均无平方因子．

例 2　全实三次域　设 $K=\mathbb{Q}(\alpha)$，α 为三次代数数，并且三个共轭元素 $\alpha^{(1)}=\alpha$，$\alpha^{(2)}$，$\alpha^{(3)}$ 均为实数(这相当于 α 的极小多项式的判别式 >0)．这时 $r_1=3$，$r_2=0$，$r=r_1+r_2-1=2$．于是 K 的基本单位组由两个单位组成．根据引理 8，我们可求出 K 的三个单位 η_1，η_2，η_3，使得

$$|\eta_j^{(i)}|\begin{cases}>1, 若\ i=j;\\ <1, 若\ i\neq j.\end{cases}\quad (1\leqslant i,\ j\leqslant 3)$$

并且引理 9 证明了这三个单位之中的任何两个都是独立的(单位组 η_1，…，η_t 叫作是独立的，是指若 $\eta_1^{a_1}\cdots\eta_t^{a_t}=1$，$a_i\in\mathbb{Z}$，则 $a_1=\cdots=a_t=0$) 我们以 ε_1 表示满足 $|\varepsilon_1^{(1)}|>1$，$|\varepsilon_2^{(1)}|<1$，$|\varepsilon_3^{(1)}|<$ 的最小者(由于满足 $|\omega^{(1)}|\leqslant|\eta_1^{(1)}|$，$|\omega^{(2)}|<1$，$|\omega^{(3)}|<1$ 的整数 $\omega\in O_K$ 只有有限个，因此上述的 ε_1 是存在的)．类似地定义 ε_2 和 ε_3．则 ε_1，ε_2 和 ε_3 中任意两个均是独立的．现在我们证明：

引理 13　满足上述条件的 ε_1，ε_2，ε_3 中任何两个都形成全实三次域 K 的基本单位组．

证明　我们首先证明：如果

$$\varepsilon_1^k\varepsilon_2^l\varepsilon_3^m=\pm 1,\ k,\ l,\ m\in\mathbb{Z},\ klm\neq 0, \qquad (*)$$

则 k，l，m 必然均为正整数．因为若不然，不妨设 $l>0$，$k<0$，$m<0$．则 $1=|\varepsilon_1^{(2)}|^k|\varepsilon_2^{(2)}|^l|\varepsilon_3^{(2)}|^m>1$ 导致矛盾，于是 k，l，m 均为正整数．现在我们设(*)式是使得 $k+l+m$ 最小的．这时 k，l，m 必然两两互素，因为若素数 $p\,|\,(l,\ m)$，则 $\varepsilon_1^k=\pm\varepsilon_2^{-l}\varepsilon_3^{-m}=\pm\eta^p$，$\eta\in U_K$．令 ξ_1，ξ_2 是域 K 的一组基本单位，则 $\varepsilon_1=\pm\xi_1^x\xi_2^y$，$\eta=\pm\xi_1^u\xi_2^v$，($x$，$y$，$u$，$v\in\mathbb{Z}$)．于是 $\xi_1^{kx}\xi_2^{ky}=\pm\xi_1^{pu}\xi_2^{pv}$，从而 $kx=pu$，$ky=pv$．由 ε_1 的极小性可知 p 不能同时除尽 x 和 y，从而 $p\,|\,k$．于是 $\varepsilon_1^{k/p}$，$\varepsilon_2^{l/p}$，$\varepsilon_3^{m/p}\in U_K$，且这三者相乘为 ± 1，这与 $k+l+m$ 的极小性相矛盾，这就表明 k，l，m 是两两互素的．最后证 $k=l=$

$m=1$；若不然，令 $l>k\geqslant m>0$，则 $\eta=\varepsilon_1\varepsilon_2\in U_K$，而 $\eta^k\varepsilon_2^{l-k}\varepsilon_3^m=\pm 1$。由 $|\varepsilon_2^{(1)}|<1$，$|\varepsilon_3^{(1)}|<1$ 可知 $|\eta^{(1)}|>1$。进而，$|\eta^{(3)}|=|\varepsilon_1^{(3)}\cdot\varepsilon_2^{(3)}|<1$。如果 $|\eta^{(2)}|<1$，则 $1<|\eta|=|\varepsilon_1\varepsilon_2|<|\varepsilon_1|$，这就与 ε_1 的极小性相矛盾。如果 $|\eta^{(2)}|>1$，则 $\left|\frac{1}{\eta}\right|<1$，$\left|\frac{1}{\eta^{(2)}}\right|<1$，从而 $\left|\frac{1}{\eta^{(3)}}\right|>1$。但是 $|1/\eta^{(3)}|^k=|\varepsilon_2^{(3)}|^{l-k}|\varepsilon_3^{(3)}|^m<|\varepsilon_3^{(3)}|^m\leqslant|\varepsilon_3^{(3)}|^k$，这也与 ε_3 的极小性相矛盾。最后，由于 $\eta^{(2)}\in\mathbb{R}$，$\eta^{(2)}\neq\pm 1$，从而 $|\eta^{(2)}|=1$ 也不可能。这就证明了 $l=k=m$，从而 $l=k=m=1$。

现在我们证明 $\varepsilon_1\varepsilon_2\varepsilon_3$ 中任意两个均形成数域 K 的基本单位组。不妨取 ε_1 和 ε_2。令 U_0 是由 ± 1，ε_1，ε_2 生成的 U_K 的子群。如果 $[U_K:U_0]>1$，则有素数 $p\mid[U_K:U_0]$，从而 U_K/U_0 有 p 阶元素 ε，即 $\varepsilon\notin U_0$，$\varepsilon^p\in U_0$，于是 $\varepsilon^p=\pm\varepsilon_1^x\varepsilon_2^y(x,\ y\in\mathbb{Z})$。令 $x=q_1p+s$，$y=q_2p+t(0\leqslant s,\ t<p)$。将 ε 改为 $\varepsilon\varepsilon_1^{-q_1}\varepsilon_2^{-q_2}$，得到 $\varepsilon\in U_K$，$\varepsilon\notin U_0$，$\varepsilon^p=\pm\varepsilon_1^s\varepsilon_2^t(0\leqslant s,\ t<p)$，显然 s，t 不全为 0。于是 $|\varepsilon^{(3)p}|=|\varepsilon_1^{(3)s}\varepsilon_2^{(3)t}|<1$，从而 $|\varepsilon^{(3)}|<1$。如果 $|\varepsilon^{(1)}|>1$，$|\varepsilon^{(2)}|<1$，则 $|\varepsilon|^p=|\varepsilon_1|^s|\varepsilon_2|^t<|\varepsilon_1|^s$，从而 $|\varepsilon|<|\varepsilon_1|$，这与 ε_1 的极小性矛盾。类似地，如果 $|\varepsilon^{(1)}|<1$，$|\varepsilon^{(2)}|>1$，则 $|\varepsilon^{(2)}|<|\varepsilon^{(2)}|$，又与 ε_2 的极小性矛盾。因此必然 $|\varepsilon^{(1)}|>1$，$|\varepsilon^{(2)}|>1$。取 $\eta=1/\varepsilon$，则 $|\eta^{(1)}|<1$，$|\eta^{(2)}|<1$，而 $1<|\eta^{(3)}|^p=|\varepsilon^{(3)}|^{-p}=|\varepsilon_1^{(3)}|^{-s}|\varepsilon_2^{(3)}|^{-t}<|\varepsilon_1^{(3)}|^{-p}\cdot|\varepsilon_2^{(3)}|^{-p}=|\varepsilon_3^{(3)}|^{-p}$，从而 $|\eta^{(3)}|<|\varepsilon_3^{(3)}|$，这又与 ε_3 的极小性矛盾，所以必然 $U_0=U_K$，这就证明了引理 11。 ▮

定义 5 设 $K/\mathbb{Q}$ 是 n 次实伽罗华扩张（从而 $r=n-1$）。$\varepsilon\in U_K$ 叫作 Minkowski 单位，是指 $\{\varepsilon^{(1)}=\varepsilon,\ \varepsilon^{(2)},\ \cdots,\ \varepsilon^{(n-1)}\}$ 形成 K 的基本单位组（由于 $\varepsilon^{(1)}\cdots\varepsilon^{(n)}=\pm 1$，这也相当于说，$\{\varepsilon^{(1)},\ \cdots,\ \varepsilon^{(n)}\}$ 中任何 $n-1$ 个均形成 K 的基本单位组）。

引理 14 设 $K/\mathbb{Q}$ 是 n 次实伽罗华扩张．则

(a) 存在 $\varepsilon\in U_K$，使得 $\{\varepsilon^{(1)}=\varepsilon,\ \varepsilon^{(2)},\ \cdots,\ \varepsilon^{(n)}\}$ 中任何 $r=n-1$ 个均是独立的；

(b) 如果 $n=p$（奇素数），则对于每个单位 $\pm 1\neq\varepsilon\in U_K$，$\{\varepsilon^{(1)},\ \cdots,\ \varepsilon^{(p)}\}$ 中任何 $p-1$ 个均是独立的；

(c) 如果 $n=3$,则 K 中存在 Minkowski 单位。

证明

(a) 设 K 为 n 次实伽罗华扩域, $G=\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_1=1, \sigma_2, \cdots, \sigma_n\}$. 由引理 8 可知存在 $\varepsilon\in U_K$, 使得 $|\sigma_1(\varepsilon)|>1$, $|\sigma_i(\varepsilon)|<1(2\leqslant i\leqslant n)$. 令 $\varepsilon_j=\sigma_j^{-1}(\varepsilon)$, 则 $|\sigma_j(\varepsilon_j)|>1$, 而 $|\sigma_i(\varepsilon_j)|<1$ (当 $i\neq j$ 时). 根据引理 9 即知 $\{\varepsilon_1, \cdots, \varepsilon_n\}=\{\varepsilon^{(1)}, \cdots, \varepsilon^{(n)}\}$ 中任何 $n-1$ 个均是独立的.

(b) 令 $G=\langle\sigma|\sigma^p=1\rangle$($G$ 必为循环群), $\pm1\neq\varepsilon\in U_K$. 如果 $\varepsilon, \sigma(\varepsilon), \cdots, \sigma^{p-2}(\varepsilon)$ 不独立, 则有不全为 0 的 $c_0, c_1, \cdots, c_{p-2}\in\mathbb{Z}$, 使得 $\varepsilon^{c_0}(\sigma(\varepsilon))^{c_1}\cdots(\sigma^{p-2}(\varepsilon))^{c_{p-2}}=\pm1$. 对于每个 $h(x)=d_0+d_1x+\cdots+d_mx^m\in\mathbb{Z}[x]$, 定义 $h(\sigma)(\varepsilon)=\varepsilon^{d_0}\sigma(\varepsilon)^{d_1}\cdots\sigma^m(\varepsilon)^{d_m}$, 则对于 $g(x)=c_0+c_1x+\cdots+c_{p-2}x^{p-2}$ 便有 $g(\sigma)(\varepsilon)=\pm1$. 但是对于 $f(x)=1+x+x^2+\cdots+x^{p-1}$ 显然有 $f(\sigma)(\varepsilon)=N(\varepsilon)=\pm1$. 因此对于 $(f(x), g(x))=h(x)$, 也有 $h(\sigma)(\varepsilon)=\pm1$(为什么?). 由于 $f(x)$ 不可约, 而 $\deg g(x)<p-1=\deg f(x)$, 从而 $h(x)=h\in\mathbb{Z}$, 即 $\varepsilon^h=\pm1$, 从而 $\varepsilon\in WK=\{\pm1\}$, 这与假设 $\varepsilon\neq\pm1$ 相矛盾, 从而 $\{\varepsilon^{(1)}, \cdots, \varepsilon^{(p-1)}, \varepsilon^{(p)}\}=\{\varepsilon, \sigma(\varepsilon), \cdots, \sigma^{p-1}(\varepsilon)\}$ 中任何 $p-1$ 个均是独立的.

(c) 设 K 为 3 次伽罗华扩张, $r=2$, 令 $K=\mathbb{Q}(\alpha)$, 考虑对数映射:

$$l: U_K\to\mathbb{R}^3, \quad l(\varepsilon)=(\log|\varepsilon^{(1)}|, \log|\varepsilon^{(2)}|, \log|\varepsilon^{(3)}|),$$

我们知道, $l(U_K)\subseteq H=\{(x_1, x_2, x_3)\in\mathbb{R}^3|x_1+x_2+x_3=0\}$. 并且 $l(U_K)$ 是 H 中的格. 令 $\pm1\neq\varepsilon\in U_K$ 使得 $l(\varepsilon)$ 是 $l(U_K)$ 中距离原点最近的(由 $l(U_K)$ 为 H 的离散子群可知这样的 ε 是存在的). 注意 $l(\varepsilon)$, $l(\varepsilon^{(2)})$, 和 $l(\varepsilon^{(3)})$ 与原点的距离相等. 而 (b) 中已证得 $\{\varepsilon, \varepsilon^{(2)}\}$ 是独立的. 从而 $l(\varepsilon)$ 和 $l(\varepsilon^{(2)})$ 是 $\mathbb{R}$-线性无关的. 记 $P=\{t_1l(\varepsilon)+t_2l(\varepsilon^{(2)})|0\leqslant t_1, t_2\leqslant1\}$, 这是以 $0=(0, 0, 0)$, $l(\varepsilon)$, $l(\varepsilon^{(2)})$ 和 $l(\varepsilon)+l(\varepsilon^{(2)})=l(\varepsilon\varepsilon^{(2)})=-l(\varepsilon^{(3)})$ 为四个顶点的平行四边形. 但是 O 与其他三个顶点距离相等, 从而 $\Delta(0, l(\varepsilon), l(\varepsilon\varepsilon^{(2)}))$ 和 $\Delta(0, l(\varepsilon^{(2)}), l(\varepsilon\varepsilon^{(2)}))$ 均为正三角形. 由 ε 的选取可知 P 内没

有 $l(U_K)$ 中的点. 另一方面, 对于每个单位 $\eta\in U_K$, $l(\eta)$ 均可表为 $l(\eta)=x_1 l(\varepsilon)+x_2 l(\varepsilon^{(2)})$, $x_i\in\mathbb{R}$. 令 $m_i=[x_i]$, $y_i=x_i-m_i$, 则 $0\leqslant y_i<1$, 于是

$$\begin{aligned} l(\eta\varepsilon^{-m_1}\varepsilon^{(2)-m_2}) &= l(\eta)-m_1 l(\varepsilon)-m_2 l(\varepsilon^{(2)}) \\ &= y_1 l(\varepsilon)+y_2 l(\varepsilon^{(2)})\in P\cap l(U_K), \end{aligned}$$

从而 $l(\eta\varepsilon^{-m_1}\varepsilon^{(2)-m_2})=0$. 即 $\eta=\pm\varepsilon^{-m_1}\varepsilon^{(2)m_2}$, $m_1, m_2\in\mathbb{Z}$. 这就表明 $\{\varepsilon, \varepsilon^{(2)}\}$ 是 K 的基本单位组, 即 ε 是 K 的 Minkowski 单位. ▌

注记 Brumer 于 1969 年证明了, 当 $p=3, 5, 7$ 等许多素数时, p 次循环域均有 Minkowski 单位. 赵春来于 1981 年给出求五次循环域 Minkowski 单位的一个好的算法. Hasse 于 1948 年给出求循环三次和四次域基本单位的算法, Gras 于 1973 年对求三次循环域的 Minkowski 单位改进了 Hasse 的算法, Gras 于 1981 年又对 Hasse 求实四次循环域的基本单位组 $(r=3)$ 改进了 Hasse 的算法. 另一种办法是从数域 K 的某些子域的单位群来决定 K 本身的基本单位组. Kulota, Wada, 张良成等人都作了这方面的工作. 但总的来讲, 计算量都是很大的.

例 3 分圆域 设 $K=\mathbb{Q}(\zeta_{p^t})$, p 为奇素数, $t\geqslant 1$. 我们已经知道, W_K 是 $2p^t$ 阶循环群.

$$n=[K:\mathbb{Q}]=\varphi(p^t),\ r_1=0,\ r_2=\frac{1}{2}\varphi(p^t),$$

从而 $r=\frac{1}{2}\varphi(p^t)-1$. 令 $K_+=\mathbb{Q}(\zeta_{p^t}+\zeta_{p^t}^{-1})$ 是 K 的极大实子域, 则 $[K_+:\mathbb{Q}]=\frac{1}{2}\varphi(p^t)$, 从而 K_+ 的基本单位组中单位的个数也是 $r=\frac{1}{2}\varphi(p^t)-1$.

引理 15 (Kummer) 分圆域 $K=\mathbb{Q}(\omega)$, $\omega=\zeta_{p^t}$ 的每个单位都是实单位和单位根的乘积.

证明 令 $G=\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_a \mid 1\leqslant a\leqslant p^t-1, p\nmid a\}$, $\sigma_a(\omega)=\omega^a$, 于是 σ_{-1} 为复共轭自同构. 对于每个 $\sigma\in G$, $\alpha\in K$, $\sigma(\bar{\alpha})=\sigma\sigma_{-1}(\alpha)=\sigma_{-1}\sigma(\alpha)=\overline{\sigma(\alpha)}$. 设 $\varepsilon\in U_K$, 则 $\bar{\varepsilon}=\sigma_{-1}(\varepsilon)\in U_K$. 并

且对于每个 $\sigma\in G$，均有 $|\sigma(\varepsilon/\bar{\varepsilon})|=|\sigma(\varepsilon)/\overline{\sigma(\varepsilon)}|=1$. 根据引理 6 即知 $\varepsilon/\bar{\varepsilon}=\lambda$ 是单位根. 但是 $W_K=\{\pm\omega^a|\ 0\leqslant a\leqslant p^t-1\}=\{\pm\omega^{2a}|0\leqslant a\leqslant p^t-1\}$，从而 $\varepsilon=\pm\omega^{2a}\bar{\varepsilon}$. 如果 $\varepsilon=\omega^{2a}\bar{\varepsilon}$，则

$$\varepsilon\cdot\omega^{-a}=\bar{\varepsilon}\omega^{a}=\overline{\varepsilon\omega^{-a}},$$

因此 $\mu=\varepsilon\cdot\omega^{-a}$ 为实单位，而 $\varepsilon=\omega^a\cdot\mu$ 即满足引理要求. 最后再证 $\varepsilon=-\omega^{2a}\bar{\varepsilon}$ 不可能. 如果 $\varepsilon=-\omega^{2a}\bar{\varepsilon}$，由于 $pO_k=\mathfrak{p}^n$，$\mathfrak{p}=(1-\omega)$，$O_K=\mathbb{Z}[\omega]$，因此 $\mu=\varepsilon\cdot\omega^{-a}=c_0+c_1\omega+\cdots+c_{n-1}\omega^{n-1}$，$c_i\in\mathbb{Z}$. $\bar{\mu}=c_0+c_1\omega^{-1}+\cdots+c_{n-1}\omega^{-(n-1)}$，但是 $\mu=-\bar{\mu}$，而

$$\omega\equiv\omega^{-1}\equiv1\ (\mathrm{mod}\ \mathfrak{p}),$$

从而 $-\mu=\bar{\mu}\equiv c_0+c_1\omega+\cdots+c_{n-1}\omega^{(n-1)}=\mu\ (\mathrm{mod}\ \mathfrak{p})$，于是 $2\mu\in\mathfrak{p}$，即 $\mu\in\mathfrak{p}$，这与 μ 是单位相矛盾. ▌

系 1 分圆域 $K=\mathbb{Q}(\zeta_{p^t})$ 中存在一组实单位

$$\{\eta_1,\ \cdots,\ \eta_r\}\left(r=\frac{1}{2}\varphi(p^t)-1\right),$$

使得它同时是 K 和其极大实子域 K_+ 的基本单位组.

证明 设 $\{\varepsilon_1,\ \cdots,\ \varepsilon_r\}$ 是 K 的任意一个基本单位组. 根据引理 15 知 $\varepsilon_i=\omega_i\eta_i$，$\omega_i\in W_K$，$\eta_i$ 为实单位，从而 η_i 也是 K_+ 中的单位. 易知这样的 $\{\eta_1,\ \cdots,\ \eta_r\}$ 满足系 1 的要求. ▌

系 2 对于分圆域 $K=\mathbb{Q}(\zeta_{p^t})$ 和它的极大实子域 K_+，我们有 $R_K/R_{K_+}=2^r$，$r=\frac{1}{2}\varphi(p^t)-1$.

证明 取 $\{\eta_1,\ \cdots,\ \eta_r\}$ 同时是 K 和 K_+ 的基本单位组(系 1). 由于 $\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_a|\ (a,\ p)=1,\ 1\leqslant a\leqslant p^t-1\}$，$\mathrm{Gal}(K_+/\mathbb{Q})=\mathrm{Gal}(K/\mathbb{Q})/\{1,\ \sigma_{-1}\}$. 从而可取

$$\{\sigma_a|1\leqslant a\leqslant\frac{1}{2}(p^t-1),\ (a,\ p)=1\}$$

为 $\mathrm{Gal}(K_+/\mathbb{Q})$ 的代表元. 于是

$$R_K=\left|\det(\lambda_a\log|\sigma_a(\eta_i)|)_{\substack{1\leqslant i\leqslant r\\ 2\leqslant a\leqslant\frac{1}{2}(p^t-1)\\ (a,p)=1}}\right|=2^r|\det(\log|\sigma_a(\eta_i)|)|$$

$$=2^rR_{K_+}.\quad ▌$$

2.4 关于费尔马猜想的 Kummer 定理

现在我们介绍 Kummer 关于费尔马猜想所作的工作. 大家知道,费尔马猜想是说:当 $n\geqslant 3$ 时,方程 $x^n+y^n=z^n$ 没有有理整数解 (x, y, z),使得 $xyz\neq 0$. 利用初等数论,不难证明这个猜想对于 $n=4$ 是正确的. 从而只需再对每个奇素数 p, 证明费尔马猜想对于 $n=p$ 正确即可(为什么?). Kummer 证明了:如果对于奇素数 p, p 不能除尽分圆域 $\mathbb{Q}(\zeta_p)$ 的类数 h_p,则费尔马猜想对于 $n=p$ 是正确的.在 100 以内除了 37, 59 和 67 之外,其余奇素数 p 均满足条件 $p\nmid h_p$, 从而对于这些奇素数 p, 费尔马猜想均正确. 自 Kummer 时代起,人们就把费尔马猜想分成两种情形,第 1 种情形是说费尔马方程 $x^p+y^p=z^p$ 不存在解满足 $p\nmid xyz\neq 0$, 第 2 种情形则是说不存在解满足 $p|xyz\neq 0$. 第 2 种情形的证明还需要应用少许 p-adic 域的知识,关于第 2 种情形的证明可参见 Боревич 和 Шафаревич 所著"数论"一书或者 L. C. Washington 的书 "Introduction to Cyclotomic Fields"第 9 章. 我们现在介绍 Kummer 对于第 1 种情形的证明. 也就是说,我们要证明:

定理 6 (Kummer) 设 p 为奇素数, h_p 是分圆域 $\mathbb{Q}(\zeta)$, $\zeta=\zeta_p$ 的类数, 如果 $p\nmid h_p$,则费尔马方程 $x^p+y^p=z^p$ 没有有理整数解 (x, y, z),使得 $p\nmid xyz\neq 0$.

证明 如果 $p=3$,由于 $3\nmid x, y, z$, 从而 x^3, y^3, $z^3\equiv\pm 1 \pmod 9$, 于是 $x^3+y^3\equiv 0$ 或者 $\pm 2\not\equiv\pm 1\equiv z^3 \pmod 9$, 这就表明定理 6 对于 $p=3$ 成立. 从而以后假设 $p\geqslant 5$. 进而, 如果 $x\equiv y\equiv -z \pmod p$,则 $x^p+y^p\equiv -2z^p$,如果 $x^p+y^p=z^p$,则 $3z^p\equiv 0 \pmod p$,但是这在 $p\geqslant 5$ 和 $p\nmid z$ 的情形下是不可能的. 因此或者 $x\not\equiv y \pmod p$,或者 $x\not\equiv -z \pmod p$,而在后一种情形下可以考虑方程 $x^p+(-z)^p=(-y)^p$. 因此我们总可以假设 $x\not\equiv y \pmod p$. 最后, 如果 $d=(x, y)$,则 $d|z$,而 $(x/d, y/d, z/d)$ 仍是费尔马方程的解. 从而我们又可设 x, y, z 两两互素.

在上述假定之下现在着手证明定理 6,在分圆域 $\mathbb{Q}(\zeta)$, $\zeta=\zeta_p$

的整数环 $\mathbb{Z}[\zeta]$ 中，方程 $x^p+y^p=z^p$ 可以写成

$$(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y)=z^p.$$

我们再证 $\mathbb{Z}[\zeta]$ 中如下三个非常简单的事实：

（一）$\mathbb{Z}[\zeta]$ 中 p 个主理想 $(x+\zeta^i y)$ $(0\leqslant i\leqslant p-1)$ 两两互素。因为若不然，则存在 $\mathbb{Z}[\zeta]$ 中一个素理想 $\mathfrak{p}$ 和 i, j, $0\leqslant i\neq j\leqslant p-1$, 使得 $x+\zeta^i y\equiv x+\zeta^j y\equiv 0(\mathrm{mod}\,\mathfrak{p})$. 从而

$$\begin{aligned}0&\equiv(x+\zeta^i y)-(x+\zeta^j y)=\zeta^i y(1-\zeta^{j-i})\\&=\zeta^i\cdot\frac{1-\zeta^{j-i}}{1-\zeta}y(1-\zeta)(\mathrm{mod}\,\mathfrak{p}).\end{aligned}$$

由于 ζ 和 $\dfrac{1-\zeta^{j-i}}{1-\zeta}$ 均为 $\mathbb{Z}[\zeta]$ 中单位，于是 $y(1-\zeta)\equiv 0(\mathrm{mod}\,\mathfrak{p})$. 另一方面，

$$0\equiv\zeta^j(x+\zeta^i y)-\zeta^i(x+\zeta^j y)=\zeta^i x(\zeta^{j-i}-1)(\mathrm{mod}\,\mathfrak{p}),$$

于是 $x(1-\zeta)\equiv 0(\mathrm{mod}\,\mathfrak{p})$. 由于已假定 $(x, y)=1$, 于是 $(1-\zeta)\equiv 0(\mathrm{mod}\,\mathfrak{p})$, 即 $\mathfrak{p}\mid(1-\zeta)$. 但是我们已经知道 $(1-\zeta)$ 是 $\mathbb{Z}[\zeta]$ 中的素理想，并且 $pO_K=(1-\zeta)^{p-1}$（见第二章）。从而必然 $\mathfrak{p}=(1-\zeta)=(1-\zeta^i)$（对每个 $1\leqslant i\leqslant p-1$）。于是 $x+y\equiv x+\zeta^i y\equiv 0$ $(\mathrm{mod}\,\mathfrak{p})$, 即 $x+y\in\mathfrak{p}\cap O_K=pO_K$. 从而 $x+y\equiv 0(\mathrm{mod}\,p)$, 于是 $z^p\equiv x^p+y^p\equiv x+y\equiv 0(\mathrm{mod}\,p)$, 即 $p\mid z$. 这与假设 $p\nmid xyz$ 相矛盾。

（二）对于每个整数 $\alpha\in\mathbb{Z}[\zeta]$, 均存在有理整数 a, 使得 $\alpha^p\equiv a(\mathrm{mod}\,p)$. 这是因为 α 可以表示为 $\alpha=a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}$, $a_i\in\mathbb{Z}$. 从而

$$\alpha^p\equiv a_0^p+a_1^p\zeta^p+\cdots+a_{p-1}^p(\zeta^{p-1})^p=a_0^p+a_1^p+\cdots+a_{p-1}^p(\mathrm{mod}\,p),$$

而同余式右方为有理整数。

（三）设 $\alpha=a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}$, $a_i\in\mathbb{Z}$. 如果至少有一个 a_i 为 0, 并且 $n\mid\alpha$, 则 n 必然除尽每个 $a_i(0\leqslant i\leqslant p-1)$. 这是由于 $\{1, \zeta, \cdots, \zeta^{p-1}\}$ 中任何 $p-1$ 个元素均形成 $\mathbb{Z}[\zeta]$ 的一组整基。

现在回到定理 6 的证明。考虑理想等式

$$\prod_{i=0}^{p-1}(x+\zeta^i y)=(z)^p,$$

根据（一），左边 p 个理想两两互素，从而每个均是某理想的 p 次

幂，即$(x+\zeta^i y)=\mathfrak{a}_i^p$ $(0\leqslant i\leqslant p-1)$. 由于左边为主理想. 因此(取$i=1$) $[\mathfrak{a}_1]^p=1$ (这里$[\mathfrak{a}]$表示理想$\mathfrak{a}$的理想类). 由于$p\nmid h_p$，即域$K=\mathbb{Q}(\zeta)$的理想类群$C(K)$中没有p阶元素，所以$[\mathfrak{a}_1]=1$，即$\mathfrak{a}_1$为主理想. 设$\mathfrak{a}_1=(\alpha)$，$\alpha\in\mathbb{Z}[\zeta]$，于是$x+\zeta y=\varepsilon\cdot\alpha^p$，其中$\varepsilon\in U_K$. 根据引理15，$\varepsilon=\zeta^r\varepsilon_1$，其中$\varepsilon_1$为实单位. 又由(二)知$\alpha^p\equiv a(\mathrm{mod}\ p)$，其中$a\in\mathbb{Z}$，从而

$$x+\zeta y=\zeta^r\varepsilon_1\alpha^p\equiv\zeta^r\varepsilon_1 a(\mathrm{mod}\,p).$$

于是$\overline{x+\zeta y}=x+\zeta^{-1}y\equiv\zeta^{-r}\varepsilon_1 a(\mathrm{mod}\,p)$. 因此

$$\zeta^{-r}(x+\zeta y)\equiv\zeta^r(x+\zeta^{-1}y)\,(\mathrm{mod}\,p),$$

即

$$x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y\equiv 0(\mathrm{mod}\,p). \qquad (*)$$

如果1, ζ, ζ^{2r}和ζ^{2r-1}两两不同，由$p\geqslant 5$和(三)可知$p|x$并且$p|y$. 这与假设$p\nmid xyz$相矛盾. 从而1, ζ, ζ^{2r}和ζ^{2r-1}至少有两个相等. 但是显然$1\neq\zeta$, $\zeta^{2r}\neq\zeta^{2r-1}$，从而只有如下三个可能.

(1) $1=\zeta^{2r}$. 此时$(*)$式变为$x+\zeta y-x-\zeta^{-1}y\equiv 0(\mathrm{mod}\,p)$，即$\zeta y-\zeta^{-1}y\equiv 0(\mathrm{mod}\,p)$. 由(三)推得$p|y$，而这与$p\nmid xyz$相矛盾.

(2) $1=\zeta^{2r-1}$，即$\zeta=\zeta^{2r}$. 这时$(*)$式变为$(x-y)-(x-y)\zeta\equiv 0(\mathrm{mod}\,p)$. 由(三)推得$x-y\equiv 0(\mathrm{mod}\,p)$，这又与假设$p\nmid(x-y)$相矛盾.

(3) $\zeta=\zeta^{2r-1}$. 这时$(*)$式为$x-\zeta^2x\equiv 0(\mathrm{mod}\,p)$. 由(三)推出$p|x$，而这又与$p\nmid xyz$相矛盾.

综合上述，我们便完全证明了定理6. ∎

注记

(1) 我们在第六章要介绍Kummer的另外一个结果. 他给出$p\nmid h_p$的一个初等判别法：$p\nmid h_p\Leftrightarrow p$除不尽Bernoulli数$B_2$, B_4, $\cdots$, B_{p-3}的分子. 令$i(p)$表示上述$\dfrac{p-3}{2}$个Bernoulli数中分子被p除尽的个数. 1972～1974年Skula, Brückner, Iwasawa将定理6推广为：如果$i(p)<\sqrt{p}-2$，则定理6的结论仍然成立

(关于 Bernoulli 数请参见第四章 § 10.4).

(2) 1978 年 Wagstaff 借助于计算机证明了，费尔马猜想(包括第 1 种情形和第 2 种情形)对于 n 为不超过 125,000 的任意奇素数均是正确的.

(3) Wieferich 给出费尔马猜想第 1 种情形的如下判别法：如果 $2^{p-1}\not\equiv 1 \pmod{p^2}$，则定理 6 的结论成立. 利用这一判别法，Lehmer 证明了对所有 $p<6\times 10^9$，定理 6 的结论均成立. 人们还猜想对于每个素数 p，均有 $2^{p-1}\not\equiv 1 \pmod{p^2}$，这一猜想目前未能完全解决.

(4) 1983 年，西德 29 岁的数学家 G. Faltings 证明了英国数学家 Mordell 于 1922 年提出的一个著名猜想. Faltings 的这项工作被誉为“本世纪最杰出的数学成就之一”. 由Faltings 的结果可以推出：对于每个奇素数 p，方程 $x^p+y^p=z^p$ 至多有有限多个整数解 $xyz\neq 0$. 这不过是 Faltings 结果许多推论当中的一个而已.

习　　题

1. 求方程 $x^2-15y^2=1$ 和 $x^2-17y^2=1$ 满足 $|x|$, $|y|\leqslant 100$ 的全部有理整数解(x, y).
2. 计算 $\mathbb{Q}(\sqrt{d})$, $d=2, 3, 5, 6, 7, 10, 11, 13, 14, 65$ 的基本单位.
3. 设 $d=t^2+4$ 无平方因子，$t\in\mathbb{Z}$, $t>0$. 求证 $\varepsilon_0=\frac{1}{2}(t+\sqrt{t^2+4})$是实二次域 $\mathbb{Q}(\sqrt{d})$的基本单位.
4. 设 $d=t^2-4$ 无平方因子，$t\geqslant 5$, $t\in\mathbb{Z}$. 求证 $\varepsilon=\frac{t+\sqrt{t^2-4}}{2}$ 为实二次域 $\mathbb{Q}(\sqrt{d})$的基本单位.
5. p 为奇素数，$K=\mathbb{Q}(\zeta)$, $\zeta=\zeta_p$. g 为模 p 的一个原根，并且 $2\nmid g$ (在 g 和 $g+p$ 中必有一个满足此条件). 令

$$\varepsilon=\zeta^{-\frac{g-1}{2}}(1-\zeta^g)/(1-\zeta)=\sin g\theta/\sin\theta,\ \ \theta=\frac{\pi}{p},$$

求证 ε 为 K 的实单位，并且 ε 的全部共轭元为

$$\varepsilon_s=\sin g^{s+1}\theta/\sin g^s\theta \quad \left(0\leqslant s\leqslant\frac{p-3}{2}\right).$$

(称 $\varepsilon=\varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{\frac{p-3}{2}}$ 为 K 中的分圆单位，我们在第六章要证明它们之中的任意 $\frac{p-3}{2}$ 个均是无关单位组.)

6. 设 $p\equiv1\pmod 4$，求证 $\mathbb{Q}(\sqrt{p})$ 的基本单位的范为 -1.

第二部分　解 析 理 论

第四章 $\zeta(s)$, $L(s,\chi)$ 和 $\zeta_K(s)$

§1 Dirichlet 级数的一般理论

在这一节里我们简略地介绍解析数论的原始思想.

1.1 Dirichlet 级数环——形式化理论

数论的一个基本课题是研究各种数论函数的性质. 所谓数论函数就是从正整数集合 $\mathbb{P}=\{1, 2, 3, \cdots\}$ 到某个带 1 交换环 R 中的映射 $f: \mathbb{P}\rightarrow R$. 如果记 $a_n=f(n)$ $(n\in P)$, 则每个取值于环 R 中的数论函数也可看成是 R 中的一个序列 $\{a_1, a_2, \cdots\}$, 多数情形下 $R=\mathbb{Z}$, 有时 R 也取为有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$ 或者复数域 $\mathbb{C}$ 等等. 下面是一些数论函数的例子.

例 1 Euler 函数 $\varphi(n)$ 定义为从 1 到 n 之中与 n 互素的整数个数. 我们知道 $\varphi(n)=n\cdot\prod_{p|n}\left(1-\frac{1}{p}\right)$.

例 2 除数函数 $d(n)=\sum_{d|n}1$, 即 $d(n)$ 为 n 的正因子个数. 例如 $d(1)=1$, $d(2)=d(3)=2$, $d(4)=3$, $d(5)=2$ 等等.

例 3 函数 $\tau(n)=\sum_{d|n}d$, 即 $\tau(n)$ 为 n 的全体正因子之和. 例如 $\tau(1)=1$, $\tau(2)=1+2=3$, $\tau(3)=1+3=4$, $\tau(4)=1+2+4=7$ 等等. 更一般地, 我们有 $\sigma_k(n)=\sum_{d|n}d^k$. 于是 $\sigma_0(n)=d(n)$, $\sigma_1(n)=\tau(n)$.

例 4 $\Omega(n)$ 为 n 的素因子个数. $\omega(n)$ 为 n 的不同素因子个数. 换句话说, 如果 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ 是 n 的素因子分解式, $p_1, \cdots, p_r$ 是不同的素数, $\alpha_i\geqslant 1$, 则 $\Omega(n)=\alpha_1+\alpha_2+\cdots+\alpha_r$, 而 $\omega(n)=r$.

例 5 $\pi(n)$ 为不超过 n 的素数的个数, 即 $\pi(n)=\sum_{p\leqslant n}1$. 例如

$\pi(2)=1$, $\pi(10)=4$, $\pi(100)=25$, $\pi(1000)=168$, $\cdots$. 对于每个数域 K, 以 $\pi(K, n)$ 表示满足 $N(\mathfrak{p})\leqslant n$ 的 K 中素理想 $\mathfrak{p}$ 的个数, 这也是数论函数.

例 6 Mangoldt 函数(log 指自然对数)

$$\Lambda(n)=\begin{cases}\log p, & \text{如果 } n=p^m,\ p \text{ 为素数}, m\geqslant 1;\\ 0, & \text{否则}.\end{cases}$$

习题中有数论函数的进一步例子.

许多数论函数之间具有"卷积"关系. 设 $f(n)$ 和 $g(n)$ 均是数论函数, 并且取值于同一个带 1 交换环 R, 所谓 $f(n)$ 和 $g(n)$ 的卷积是指一个新的数论函数 $h: \mathbb{P}\to R$, 它在每个 $n\in P$ 处的取值为

$$h(n)=\sum_{d\mid n}f(d)g(n/d).$$

我们记成 $h=f*g$. 例如容易验证: $\{d(n)\}=\{1\}*\{1\}$, $\{\sigma_k(n)\}=\{1\}*\{n^k\}$, $\{\Lambda(n)\}*\{1\}=\{\log n\}$, $\{n\}=\{1\}*\{\varphi(n)\}$等等, 其中 $\{1\}$表示恒等于 1 的函数.

对于每个数论函数 $f: \mathbb{P}\to R$, 我们结合一个表达式

$$F(s)=\sum_{n=1}^{\infty}f(n)/n^s=\frac{f(1)}{1^s}+\frac{f(2)}{2^s}+\cdots+\frac{f(n)}{n^s}+\cdots$$

称作是数论函数 f 的形式 Dirichlet 级数, 简称作形式 D-级数(所谓"形式"一词的含义, 即指我们只不过是把级数 $F(s)$中的 s 看作是符号而已). 反过来, 每个环 R 上的形式 D-级数

$$F(s)=\sum_{n=1}^{\infty}a_n/n^s \quad (a_n\in R)$$

也对应着一个数论函数 $f: \mathbb{P}\to R$, $f(n)=a_n$. 如果我们定义两个形式 D-级数 $\sum_{n=1}^{\infty}a_n/n^s$ 和 $\sum_{n=1}^{\infty}b_n/n^s$ 相等, 当且仅当 $a_n=b_n$ $(n=1, 2, \cdots)$, 那末数论函数与它的形式 D-级数(以及 R 中的序列 $\{a_1, a_2, \cdots\}$)之间建立起一一对应关系. 进而, 对于两个形式 D-级数 $F(s)=\sum_{n=1}^{\infty}a_n/n^s$ 和 $G(s)=\sum_{n=1}^{\infty}b_n/n^s$, 我们将它们"形式"地相加和相乘(并且合并同类项), 即

$$F(s)+G(s)=\sum_{n=1}^{\infty}(a_n+b_n)/n^s,$$

$$F(s)G(s)=\sum_{r=1}^{\infty}\sum_{k=1}^{\infty}a_rb_k/r^sk^s=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{rk=n}a_rb_k$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{d|n}a_db_{n/d}.$$

这表明：形式 D-级数的形式加法对应着数论函数的通常加法，而形式 D-级数的形式乘法恰好对应着数论函数的卷积！以 $D(R)$ 表示带 1 交换环 R 上全体形式 D-级数所构成的集合，即

$$D(R)=\left\{\sum_{n=1}^{\infty}a_n/n^s \mid a_n\in R,\ n=1,\ 2,\ 3,\ \cdots\right\}.$$

$D(R)$ 对于形式加法和乘法显然形成带 1 交换环，其零元素和幺元素分别为 0 和 1. $D(R)$ 称作是 R 上的形式 D-级数环. 如果以 $R^{\mathbb{P}}$ 表示取值于环 R 的全部数论函数所构成的集合，即

$$R^{\mathbb{P}}=\{f:\mathbb{P}\to R\}.$$

根据上述对应关系我们就知道，$R^{\mathbb{P}}$ 对于通常加法和卷积乘法也形成带 1 交换环，其零元素是恒为 0 的函数，而幺元素为数论函数 $e(n)$，其中 $e(1)=1$，$e(n)=0$（当 $n\geqslant 2$ 时），称 $(R^{\mathbb{P}},\ +,\ *)$ 为 $\boldsymbol{R}$ **上的数论函数环**. 环 $D(R)$ 和 $R^{\mathbb{P}}$ 是同构的. 基于这一同构，$D(R)$ 和 $R^{\mathbb{P}}$ 中任何一个环中的性质都可翻译成另一个环中一个对应的性质. 下面就是环 $D(R)$ 中的一些简单性质.

引理 1 (a) 若 R 为整环，则 $D(R)$ 也是整环.

(b) $\sum_{n=1}^{\infty}a_n/n^s$ 为 $D(R)$ 中的单位 $\Leftrightarrow$ a_1 为 R 中的单位. 并且若 a_1 是 R 中的单位，令 $\sum_{n=1}^{\infty}b_n/n^s$ 是 $\sum_{n=1}^{\infty}a_n/n^s$ 的逆元素，则诸系数 b_n 可如下递归地求出：

$$b_1=a_1^{-1},\ b_n=-a_1^{-1}\sum_{\substack{d|n\\ d\neq 1}}a_d\cdot b_{n/d}\quad(n\geqslant 2).$$

证明 (a) 设 $F(s)=\sum_{n=1}^{\infty}a_n/n^s$，$G(s)=\sum_{n=1}^{\infty}b_n/n^s$. 如果 $F(s)\neq 0$，$G(s)\neq 0$，则存在 n_1，n_2 使得 $a_1=\cdots=a_{n_1-1}=b_1=\cdots=b_{n_2-1}=0$，$a_{n_1}\neq 0$，$b_{n_2}\neq 0$. 于是

$$F(s)G(s)=\left(\sum_{n=n_1}^{\infty} a_n/n^s\right)\cdot\left(\sum_{n=n_2}^{\infty} b_n/n^s\right)=\sum_{n=n_1n_2}^{\infty} c_n/n^s,$$

$c_{n_1n_2}=a_{n_1}b_{n_2}$. 由于 R 为整区，从而 $c_{n_1n_2}=a_{n_1}b_{n_2}\neq 0$，于是 $F(s)G(s)\neq 0$，即 $D(R)$ 也是整环.

(b) 如果 $\sum\limits_{n=1}^{\infty}a_n/n^s$ 为环 $D(R)$ 中单位，则有 $\sum\limits_{n=1}^{\infty}b_n/n^s\in D(R)$，使得 $\left(\sum\limits_{n=1}^{\infty} a_n/n^s\right)\left(\sum\limits_{n=1}^{\infty} b_n/n^s\right)=1$. 于是 $1=a_1b_1$，$0=\sum\limits_{d|n}a_d\cdot b_{n/d}$ $(n\geqslant 2)$，从而 a_1 为环 R 中单位，$b_1=a_1^{-1}$. 并且当 $n\geqslant 2$ 时 $a_1b_n+\sum\limits_{\substack{d|n\\ d\neq 1}}a_d\cdot b_{n/d}=0$，即

$$b_n=-a_1^{-1}\sum_{\substack{d|n\\ d\neq 1}}a_d\cdot b_{n/d}. \tag{*}$$

反过来，如果 a_1 为 R 中单位，取 $b_1=a_1^{-1}$，然后由(*)式递归地求出 $b_n(n\geqslant 2)$. 不难证明 $\sum\limits_{n=1}^{\infty}b_n/n^s$ 是 $\sum\limits_{n=1}^{\infty}a_n/n^s$ 的逆元素. ∎

例 取 $R=\mathbb{Z}$，恒等于 1 的数论函数所对应的形式 D-级数就是著名的 **Riemann zeta 函数**

$$\zeta(s)=\sum_{n=1}^{\infty}1/n^s.$$

由引理 1 知它是环 $D(R)$ 中乘法可逆元素. 假设其逆为

$$\zeta^{-1}(s)=\sum_{n=1}^{\infty}\mu(n)/n^s.$$

$\zeta^{-1}(s)$ 对应的数论函数 $\{\mu(n)\}$ 称作是 Möbius 函数. 将 $\zeta(s)\cdot\zeta^{-1}(s)=1$ 翻译到数论函数环 $\mathbb{Z}^{\mathbb{P}}$ 上就是 $\{1\}*\{\mu(n)\}=e$，这可写成

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1\text{ 时};\\ 0, & n\geqslant 2\text{ 时}.\end{cases}$$

因此我们可递归求出 $\mu(n)$ 的数值：

$$\mu(1)=1,\quad \mu(n)=-\sum_{\substack{d|n\\ d\neq 1}}\mu(n/d)=-\sum_{\substack{d|n\\ d\neq n}}\mu(d).$$

由此可求出 $\mu(2)=-1$，$\mu(3)=-1$，$\mu(4)=0$，$\mu(5)=-1$，$\mu(6)=1$ 等等. 但是我们希望能求出 $\mu(n)$ 的明显表达式. 这需要新

的概念以及环 $R^{\mathbb{P}}$ 和 $D(R)$ 之间的进一步联系.

定义 1 数论函数 f 叫作是积性的，是指当 $(m, n)=1$ 时 $f(mn)=f(m)f(n)$. f 叫作是完全积性的，是指对任何 $m, n\in\mathbb{P}$，均有 $f(mn)=f(m)f(n)$.

若 $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ 是 n 的素因子分解式，其中 $p_1, \cdots, p_r$ 为不同的素数，$\alpha_i\geqslant 1$. 由上述定义不难归纳证出:

(a) 如果 f 是积性数论函数，则 $f(1)=1$ 并且

$$f(n)=\prod_{i=1}^{r} f(p_i^{\alpha_i});$$

(b) 如果 f 是完全积性数论函数，则

$$f(n)=\prod_{i=1}^{r} f(p_i)^{\alpha_i}.$$

这表明：每个积性数论函数由它在所有素数幂 p^α 处的值所完全决定，而完全积性数论函数由它在所有素数处的取值所完全决定. 环 $R^{\mathbb{P}}$ 中的这些事实自然要反映到环 $D(R)$ 中来，这就是:

引理 2 设 $F(s)$ 是数论函数 $f(n)$ 的形式 D-级数.

(a) f 为积性的 $\Leftrightarrow$ $F(s)$ 有如下的 Euler 乘积展开式

$$F(s)=\prod_p(1+f(p)p^{-s}+f(p^2)p^{-2s}+\cdots+f(p^m)p^{-ms}+\cdots)$$

$$=\prod_p\left(\sum_{m=0}^{\infty}f(p^m)/p^{ms}\right).$$

(b) f 为完全积性的 $\Leftrightarrow$ $F(s)$ 有如下的 Euler 乘积展开式

$$F(s)=\prod_p(1-f(p)p^{-s})^{-1}.$$

证明 (我们在证明中也同时解释如何将上述 Euler 乘积展开式看成是形式 D-级数). 对于(a)中的 Euler 乘积，p 过全部素数. 从而这是无限个形式 D-级数

$$F_p(s)=1+f(p)p^{-s}+f(p^2)p^{-2s}+\cdots+f(p^m)p^{-ms}+\cdots$$
$$(p^{-ms}=1/p^{ms})$$

的乘积. 对于每个正整数 $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，乘积 $F(s)$ 中只有一项以 n^s 为分母，那就是在因子 $F_{p_i}(s)$ 中取 $f(p_i^{\alpha_i})p_i^{-\alpha_i s}$ $(1\leqslant i\leqslant r)$，而在其余因子 $F_p(s)$ 中均取第一项 1 然后相乘而得到的 $f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r})n^{-s}$.

用这种方法决定出每项 $c_n n^{-s}$ 的系数 c_n，从而 (a)中的 Euler 乘积 $F(s)$可看成是形式 D-级数. 并且它是 f 的形式 D-级数 $\Leftrightarrow$ $f(p_1^{\alpha_1}\cdots p_r^{\alpha_r})=f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r})\Leftrightarrow f$ 为积性函数.

类似地，在(b)中将$(1-f(p)p^{-s})^{-1}$ 作为可逆元素 $1-f(p)p^{-s}$ 的逆，易知是 $(1-f(p)p^{-s})^{-1}=1+f(p)p^{-s}+f(p)^2p^{-2s}+\cdots+f(p)^m p^{-ms}+\cdots$. 从而 $F(s)=\prod\limits_p(1-f(p)p^{-s})^{-1}$ 为 f 的形式 D-级数 $\Leftrightarrow f(p_1^{\alpha_1}\cdots p_r^{\alpha_r})=f(p_1)^{\alpha_1}\cdots f(p_r)^{\alpha_r}\Leftrightarrow f$ 是完全积性函数. ▮

恒等于1的数论函数$\{1\}$显然是完全积性的，从而它的形式 D-级数 $\zeta(s)$有如下的 Euler 乘积展开式:

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}=\prod_p(1-p^{-s})^{-1}.$$

于是它的逆为

$$\zeta^{-1}(s)=\sum_{n=1}^{\infty}\mu(n)n^{-s}=\prod_p(1-p^{-s}).$$

由此我们得到 Möbius 函数 $\mu(n)$的明显表达式:

$$\mu(n)=\begin{cases}1, & \text{当 } n=1 \text{ 时;}\\ (-1)^r, & \text{如果 } n \text{ 为 } r \text{ 个不同的素数之乘积;}\\ 0, & \text{否则.}\end{cases}$$

引理 3 (Möbius 反演公式) 设 f 和 g: $\mathbb{P}\to R$ 是两个数论函数. 则

$$f(n)=\sum_{d|n}g(d)\ (n=1,\ 2,\ \cdots)\Leftrightarrow g(n)=\sum_{d|n}f(d)\mu(n/d)\quad(n=1,\ 2,\ \cdots).$$

证明 设 $F(s)$和 $G(s)$分别是 f 和 g 的形式 D-级数，则

上式左边 $\Leftrightarrow f=g*\{1\}\Leftrightarrow F(s)=G(s)\zeta(s)\Leftrightarrow G(s)=F(s)\zeta^{-1}(s)\Leftrightarrow g=f*\mu\Leftrightarrow$ 上式右边. ▮

利用以上这些简单的引理，我们能够求出不少数论函数的形式 D-级数. 值得注意的是，这些形式 D-级数有许多均可用 Riemann zeta 函数 $\zeta(s)$表达出来.

例 1 函数$\{f(n)=n^k\}$的形式 D-级数 显然是

$$F(s)=\sum_{n=1}^{\infty} n^k/n^s=\sum_{n=1}^{\infty}1/n^{s-k}=\zeta(s-k).$$

例 2 对于函数 $\sigma_k(n)=\sum_{d|n} d^k$，则 $\sigma_k=\{n^k\}*\{1\}$. 因此 σ_k 的形式 D–级数为 $\zeta(s)\zeta(s-k)$. 特别地，除数函数 $d(n)=\sum_{d|n}1$ 的形式 D–级数为 $\zeta(s)^2$，而函数 $\tau(n)=\sum_{d|n}d$ 的形式 D 级数为 $\zeta(s)\zeta(s-1)$.

例 3 Euler 函数 $\varphi(n)$ 熟知为积性函数，并且 $\varphi(p^m)=p^m-p^{m-1}$，从而它的形式 D–级数为

$$\begin{aligned}\sum_{n=1}^{\infty}\varphi(n)/n^s&=\prod_p\left(1+\frac{p-1}{p^s}+\frac{p^2-p}{p^{2s}}+\cdots+\frac{p^m-p^{m-1}}{p^{ms}}+\cdots\right)\\&=\prod_p(1-p^{-s})(1-p^{-(s-1)})^{-1}=\zeta(s-1)/\zeta(s).\end{aligned}$$

于是 $\zeta(s-1)=\zeta(s)\cdot\sum\varphi(n)n^{-s}$. 由此得到 $\sum_{d|n}\varphi(d)=n$. 当然我们也可以用初等方法直接证明 $\sum_{d|n}\varphi(d)=n$，然后立即得到

$$\sum\varphi(n)n^{-s}=\zeta(s-1)/\zeta(s).$$

进一步的例子请见习题.

以上我们通过数论函数与其形式 D–级数之间的对应，得到许多数论函数之间的关系和恒等式. 但是，作为数论的主要目标是研究各种数论函数 $\{f(n)\}$ 的性状，例如 $f(n)$ 的大小或者其均值 $A(x)=\sum_{n<x}f(n)$ 的大小等等. 为了作到这一点，只研究“形式”D–级数就不够了. 我们要将数论函数 $f(n)$ 的 D–级数 $\sum f(n)n^{-s}$ 看成是 $s\in\mathbb{C}$ 的复变函数，从而引入解析工具. 正是在这一点上，Dirichlet 和 Riemann 等人将数论和复变函数论结合起来，开创了一门富有成果的学科——解析数论.

1.2 收敛横坐标——解析工具的引入

从现在开始，我们将数论函数 $f(n)=a_n\ (a_n\in\mathbb{C})$ 的 D–级数 $F(s)=\sum_{n=1}^{\infty}a_nn^{-s}$ 看作是复变函数，$s=\sigma+it\in\mathbb{C}$, σ, $t\in\mathbb{R}$. 下面

定理表明 $F(s)$ 的解析性质与数论函数 $f(n)=a_n$ 的部分和 $A(N)=\sum_{n=1}^{N}a_n$ 的大小有密切联系.

定理 1 设 $F(s)=\sum_{n=1}^{\infty}a_n n^{-s}$, $a_n\in\mathbb{C}$, $s=\sigma+it\in\mathbb{C}$, $A(N)=\sum_{n=1}^{N}a_n$. 则

(a) 存在 σ_0, $-\infty\leqslant\sigma_0\leqslant+\infty$, 使得当 $\sigma>\sigma_0$ 时, 级数 $F(s)$ 收敛, 并且在右半开平面 $\sigma>\sigma_0$ 的每个紧子集内均一致收敛. 而当 $\sigma<\sigma_0$ 时级数 $F(s)$ 发散.

(b) 级数 $F(s)$ 定义出右半开平面 $\sigma>\sigma_0$ 中的正则函数, 并且可以逐项微商.

(c) 如果 $\{A(N)\,|\,N=1, 2, \cdots\}$ 发散, 则

$$\sigma_0=\inf\{\alpha\,|\,A(N)=O(N^{\alpha})\}=\overline{\lim_{N\to\infty}}\log|A(N)|/\log N.$$

注记 定理 1 中的 σ_0 称作是级数 $F(s)$ 的收敛横坐标.

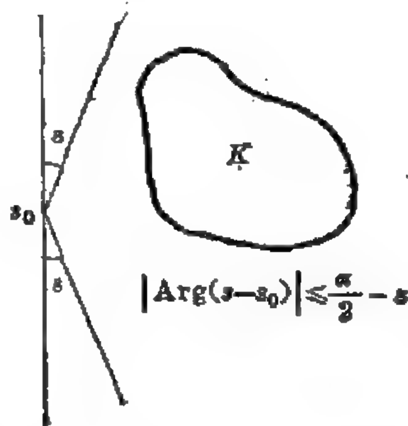
证明 (a)和(b). 我们要证: 如果级数 $F(s)$ 在 $s=s_0$ 处收敛, 则当 $\mathrm{Re}(s)>\mathrm{Re}(s_0)$ 时级数 $F(s)$ 也收敛, 并且在右半开平面 $\mathrm{Re}(s)\geqslant\sigma$ (对任意的 $\sigma>\mathrm{Re}(s_0)$) 内一致收敛. 由此不难得出收敛横坐标 σ_0 的存在性: $\sigma_0=\inf\{\mathrm{Re}(s)\,|$ 级数 $F(s)$ 在 s 处收敛$\}$, 并且再由 Weierstrass 一致收敛定理即得到(b)中结果.

给了右半平面

$$\mathrm{Re}(s)\geqslant\sigma \quad (\sigma>\mathrm{Re}(s_0))$$

中的一个紧子集 K, 不难看出, 存在 $\varepsilon>0$, 使得 K 包含在区域

$$|\mathrm{Arg}(s-s_0)|\leqslant\frac{\pi}{2}-\varepsilon$$



之中. 我们现在证明级数 $F(s)$ 在这个区域中一致收敛. 必要时将 s 改成 $s-s_0$, a_n 改成 $a_n n^{s_0}$, 我们可以不妨假设 $s_0=0$. 这时 $F(0)=\sum_{n=1}^{\infty}a_n$ 收敛. 令 $A(M, N)=\sum_{n=M}^{N}a_n$, 则对预先给定的 $\varepsilon>0$, 存在 N_0, 使

得当 $N>M\geqslant N_0$ 时，$|A(M,N)|\leqslant\varepsilon$ 于是

$$\begin{aligned}\sum_{n=M}^{N}a_nn^{-s}&=\sum_{n=M}^{N}(A(M,n)-A(M,n-1))n^{-s}\\&=\sum_{n=M}^{N-1}A(M,n)[n^{-s}-(n+1)^{-s}]\\&\quad+A(M,N)N^{-s}.\end{aligned}$$

但是

$$\begin{aligned}|n^{-s}-(n+1)^{-s}|&=\left|s\int_n^{n+1}x^{-(s+1)}\mathrm{d}x\right|\leqslant|s|\int_n^{n+1}x^{-(\sigma+1)}\mathrm{d}x\\&=\frac{|s|}{\sigma}(n^{-\sigma}-(n+1)^{-\sigma}).\end{aligned}$$

而在 $|\mathrm{Arg}(s)|\leqslant\frac{\pi}{2}-\varepsilon$ 中 $\frac{|s|}{\sigma}$ 是有界的. 从而对于 $\sigma>0$ 有

$$\begin{aligned}\left|\sum_{n=M}^{N}a_nn^{-s}\right|&\leqslant\sum_{n=M}^{N-1}|A(M,n)|(n^{-\sigma}-(n+1)^{-\sigma})\\&\quad+|A(M,N)|N^{-\sigma}\\&\leqslant C\varepsilon\sum_{n=M}^{N-1}(n^{-\sigma}-(n+1)^{-\sigma})+\varepsilon N^{-\sigma}\\&\leqslant C\varepsilon M^{-\sigma}+\varepsilon N^{-\sigma}\leqslant(C+1)\varepsilon N_0^{-\sigma}.\end{aligned}$$

这就证明了 $F(s)$ 在区域 $|\mathrm{Arg}(s)|\leqslant\frac{\pi}{2}-\varepsilon$ 中从而在 K 中一致收敛.

(c) 令 $\gamma=\inf\{\alpha|A(N)=O(N^\alpha)\}$. 先证 $\gamma\leqslant\sigma_0$: 对于每个 $\sigma>\sigma_0$, 由(a)知 $\sum a_nn^{-\sigma}$ 收敛. 由于假设 $A(N)=\sum_{n=1}^{N}a_n$ 发散，从而 $\sigma_0\geqslant0$, 于是 $\sigma>0$. 因此

$$\begin{aligned}|A(N)|&=\left|\sum_{n=1}^{N}(a_nn^{-\sigma})n^{\sigma}\right|\\&=\left|\sum_{n=1}^{N}\left(\sum_{m=1}^{n}a_mm^{-\sigma}-\sum_{m=1}^{n-1}a_mm^{-\sigma}\right)n^{\sigma}\right|\\&=\left|\sum_{n=1}^{N-1}\left(\sum_{m=1}^{n}a_mm^{-\sigma}\right)(n^{+\sigma}-(n+1)^{+\sigma})\right.\\&\quad\left.+\left(\sum_{n=1}^{N}a_nn^{-\sigma}\right)N^{\sigma}\right|\end{aligned}$$

$$\leqslant \sum_{n=1}^{N-1}\left|\sum_{m=1}^{n} a_m m^{-\sigma}\right|((n+1)^{\sigma}-n^{\sigma})$$
$$+\left|\sum_{n=1}^{N} a_n n^{-\sigma}\right|\cdot N^{\sigma}$$
$$<C\sum_{n=1}^{N-1}((n+1)^{\sigma}-n^{\sigma})+CN^{\sigma}<2CN^{\sigma}.$$

从而 $A(N)=O(N^{\sigma})$. 由 γ 的定义可知 $\gamma\leqslant\sigma$, 因此 $\gamma\leqslant\sigma_0$.

反之, 如果 $\sigma>\gamma$, 则

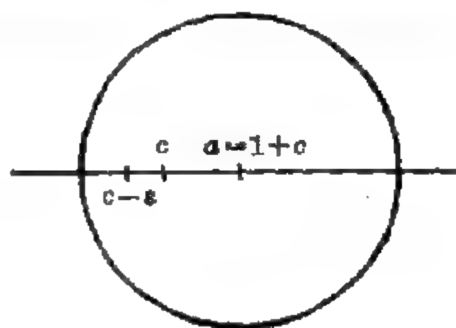
$$\sum_{n=1}^{N} a_n n^{-\sigma}=\sum_{n=1}^{N-1} A(n)(n^{-\sigma}-(n+1)^{-\sigma})+A(N)N^{-\sigma}. \qquad (*)$$

取 α 使得 $\gamma<\alpha<\sigma$, 再取常数 C 使得 $|A(N)|\leqslant CN^{\alpha}$(对于所有的 N). 于是

$$|A(n)(n^{-\sigma}-(n+1)^{-\sigma})|\leqslant Cn^{\alpha}(n^{-\sigma}-(n+1)^{-\sigma})$$
$$=C\sigma n^{\alpha}\int_{n}^{n+1} x^{-\sigma-1}\,dx<c\sigma n^{\alpha-\sigma-1}.$$

由于 $|A(N)N^{-\sigma}|\leqslant CN^{\alpha-\sigma}\to 0$ 而 $\sum\limits_{n=1}^{\infty} n^{\alpha-\sigma-1}$ 收敛, 从而由(*)式可知 $\lim\limits_{N\to\infty}\sum\limits_{n=1}^{N} a_n n^{-\sigma}$ 存在. 于是 $\sigma_0\leqslant\sigma$, 从而 $\sigma_0\leqslant\gamma$. ∎

定理 2 (Landau) 设 $a_n\geqslant 0\,(n=1, 2, \cdots)$, 级数 $F(s)=\sum\limits_{n=1}^{\infty} a_n n^{-s}$ 在半平面 $\mathrm{Re}(s)>c$ 中收敛. 如果函数 $F(s)$ 在以 $s=c$ 为中心的一个小圆内解析, 则有 $\varepsilon>0$ 使级数 $\sum\limits_{n=1}^{\infty} a_n n^{-s}$ 在半平面 $\mathrm{Re}(s)>c-\varepsilon$ 内收敛. 特别地, 若 σ_0 为级数 $\sum\limits_{n=1}^{\infty} a_n n^{-s}$ 的收敛横坐标, 则函数 $F(s)$ 在 $s=\sigma_0$ 处为奇点.



证明 令 $a=1+c$, 由于函数 $F(s)$ 在 $s=a$ 处解析, 从而有 Taylor 展开

$$F(s)=\sum_{k=0}^{\infty}\frac{F^{(k)}(a)}{k!}(s-a)^{k},$$

并且此 Taylor 级数在 a 附近绝对收敛. 因为 $F(s)$ 在 c 处解析, 从而收敛半径超过 1. 将 $F(s)=\sum a_n n^{-s}$ 逐项微商得到

$$F^{(k)}(s)=(-1)^k\sum_{n=1}^{\infty}a_n(\log n)^k n^{-s},$$

从而 $F(s)=\sum_{k=0}^{\infty}\sum_{n=1}^{\infty}\frac{(a-s)^k}{k!}a_n(\log n)^k n^{-a}$. 因为收敛半径>1, 此式对某个 $s=c-\varepsilon$ 成立($\varepsilon>0$). 而 $a-s=1+\varepsilon$. 由于上面二重级数每项均$\geqslant 0$, 从而可变换求和次序, 得到

$$F(c-\varepsilon)=\sum_{n=1}^{\infty}\frac{a_n}{n^a}\sum_{k=1}^{\infty}\frac{((1+\varepsilon)\log n)^k}{k!}$$

$$=\sum_{n=1}^{\infty}\frac{a_n}{n^a}e^{(1+\varepsilon)\log n}=\sum_{n=1}^{\infty}\frac{a_n}{n^{c-\varepsilon}},$$

即 $\sum a_n n^{-s}$ 在 $s=c-\varepsilon$ 处收敛, 从而由定理1知它在 $\mathrm{Re}(s)>c-\varepsilon$ 中均收敛. ∎

例1 对于 $a_n=1(n=1, 2, \cdots)$, $A(N)=N\to\infty$. 由定理1(c)可知 Riemann zeta函数 $\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$ 的收敛横坐标为 $\sigma_0=1$, 从而级数 $\zeta(s)$ 在右半平面 $\mathrm{Re}(s)>1$ 中定义出一个正则函数. 而由定理2知道 $s=1$ 是 $\zeta(s)$ 的奇点.

例2 对于 $a_n=(-1)^n$, $A(N)=\begin{cases}-1, & 2\nmid N;\\ 0, & 2\mid N.\end{cases}$ 从而$\{A(N)\mid N=1, 2, \cdots\}$发散. 由定理1(c)可知级数 $F_2(s)=\sum_{n=1}^{\infty}(-1)^n n^{-s}$ 的收敛横坐标 $\sigma_0=0$. 这表明 $F_2(s)$ 在 $s=1$ 处正则. 但是

$$F_2(s)=\sum_{n=1}^{\infty}(-1)^n n^{-s}=-\sum_{n=1}^{\infty}n^{-s}+2\sum_{n=1}^{\infty}(2n)^{-s}$$

$$=-(1-2^{-(s-1)})\zeta(s)\quad(\mathrm{Re}(s)>1).$$

而在 $s=1$ 处, $(1-2^{-(s-1)})=(s-1)\log 2+(s-1)^2a+\cdots$, 这就表明 $\zeta(s)$ 在 $s=1$ 处是单极点, 并且留数是

$$\operatorname*{res}_{s=1}\zeta(s)=-F_2(1)/\log 2=-\frac{1}{\log 2}\left(-1+\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-\cdots\right)$$

$$=\log 2/\log 2=1.$$

此外, $\zeta(s)$ 在半平面 $\mathrm{Re}(s)>0$ 内的其他奇点只可能是

$$s=1+\frac{2\pi i n}{\log 2}\quad(n\in\mathbb{Z}).$$

例 3 令 $w=e^{2\pi i/3}$, $F_3(s)=\sum_{n=1}^{\infty}w^n n^{-s}$, $\overline{F}_3(s)=\sum_{n=1}^{\infty}w^{2n}n^{-s}$. 由于 $w+w^2+1+w+w^2+1+\cdots$ 是发散的并且部分和有界, 从而 $F_3(s)$ 和 $\overline{F}_3(s)$ 的收敛横坐标均为 $\sigma_0=0$. 但是

$$\zeta(s)+F_3(s)+\overline{F}_3(s)=\sum_{n=1}^{\infty}(1+w^n+w^{2n})n^{-s}$$

$$=3\cdot\sum_{n=1}^{\infty}(3n)^{-s}=3^{1-s}\zeta(s),$$

即 $-(1-3^{1-s})\zeta(s)=F_3(s)+\overline{F}_3(s)$. 从而 $\zeta(s)$ 除了 $s=1$ 之外在 $\mathrm{Re}(s)>0$ 内的极点只能是 $1+2\pi in/\log 3$. 但是 $\log 2/\log 3$ 是无理数, 即不存在 $(n, n')\neq(0, 0)$, 使得

$$1+2\pi in/\log 2=1+2\pi in'/\log 3,$$

这就表明 $\zeta(s)$ 可用公式

$$\zeta(s)=-(1-2^{-(s-1)})^{-1}F_2(s)$$

或
$$\zeta(s)=-(1-3^{-(s-1)})^{-1}(F_3(s)+\overline{F}_3(s))$$

解析延拓到半平面 $\mathrm{Re}(s)>0$ 之中, 并且在此区域中只有 $s=1$ 为 $\zeta(s)$ 的奇点(而且是留数为 1 的单极点).

定义 2 D-级数 $\sum|a_n|n^{-s}$ 的收敛横坐标 σ_1 叫作是级数 $\sum a_n n^{-s}$ 的**绝对收敛横坐标**. 显然 $\sigma_1\geqslant\sigma_0$. 另一方面, 可以证明 $\sigma_1\leqslant\sigma_0+1$(习题).

我们在上一小节中看到, 当 $\{f(n)=a_n\}$ 为积性函数时, 它的形式 D-级数(作为环 $D(R)$ 中的元素)可表成 Euler 积的形式. 现在我们要证明, 当 $R=\mathbb{C}$ 而把它们看成是复变函数时也是相等的.

定理 3 设 $f:\mathbb{P}\to\mathbb{C}$ 是积性数论函数, σ_1 为级数 $\sum f(n)n^{-s}$ 的绝对收敛横坐标. 则当 $\mathrm{Re}(s)>\sigma_1$ 时, 无穷乘积

$$\prod_p(1+f(p)p^{-s}+\cdots+f(p^m)p^{-ms}+\cdots)$$

绝对收敛, 并且等于 $\sum_{n=1}^{\infty}f(n)n^{-s}$.

证明 考虑有限乘积

$$P(x)=\prod_{p<x}(1+f(p)p^{-s}+\cdots+f(p^m)p^{-ms}+\cdots).$$

当 $\mathrm{Re}(s)>\sigma_1$ 时，这是有限个绝对收敛级数的乘积，从而展开式逐项可任意交换次序．每项有形式 $f(p_1^{\alpha_1}\cdots p_r^{\alpha_r})(p_1^{\alpha_1}\cdots p_r^{\alpha_r})^{-s}$．从而

$$p(x)=\sum_{n\in A_x}f(n)n^{-s},\quad A_x=\{n\,|\,n\text{ 的素因子均 }\leqslant x\},$$

于是 $\sum\limits_{n=1}^{\infty}f(n)n^{-s}-P(x)=\sum\limits_{n\in B_x}f(n)n^{-s}$，$B_x=\{n\,|\,n\text{有素因子 }p>x\}$．从而当 $x\to\infty$ 时，

$$\left|\sum_{n=1}^{\infty}f(n)n^{-s}-P(x)\right|\leqslant\sum_{n\in B_x}|f(n)n^{-s}|\leqslant\sum_{n>x}|f(n)n^{-s}|\to 0.$$

这就表明 $P(x)\to\sum\limits_{n=1}^{\infty}f(n)n^{-s}$．另一方面，从微积分我们知道，无穷乘积 $\prod\limits_{n=1}^{\infty}(1+\alpha_n)\,(\alpha_n\in\mathbb{C})$ 的绝对收敛性是 $\sum\limits_{n=1}^{\infty}\alpha_n$ 绝对收敛性的直接推论．在我们这里，由于

$$\begin{aligned}&\sum_{p\leqslant x}|f(p)p^{-s}+\cdots+f(p^m)p^{-ms}+\cdots|\\&\quad\leqslant\sum_{p\leqslant x}(|f(p)p^{-s}|+\cdots+|f(p^m)p^{-ms}|+\cdots)\\&\quad\leqslant\sum_{n=2}^{\infty}|f(n)n^{-s}|,\end{aligned}$$

这就表明无穷乘积 $\prod\limits_{p}(1+f(p)p^{-s}+\cdots+f(p^m)p^{-ms}+\cdots)$ 在 $\mathrm{Re}(s)>\sigma_1$ 时是绝对收敛的． ∎

注记

1．完全类似地，如果 $f(n)$ 是完全积性函数，则当 $\mathrm{Re}(s)>\sigma_1$ 时（σ_1 为 $\sum f(n)n^{-s}$ 的绝对收敛横坐标）

$$\sum_{n=1}^{\infty}f(n)n^{-s}=\prod_{p}(1-f(p)p^{-s})^{-1}.$$

例如，作为复变函数，当 $\mathrm{Re}(s)>1$ 时，$\zeta(s)=\prod\limits_{p}(1-p^{-s})^{-1}$，而当 $\mathrm{Re}(s)>2$ 时，$\sum\varphi(n)n^{-s}=\zeta(s-1)/\zeta(s)=\prod\limits_{p}(1-p^{-s})(1-p^{1-s})^{-1}$ 等等．

2．以上我们是从数论函数 $f(n)=a_n\left(\text{或者 }A(N)=\sum\limits_{n=1}^{N}a_n\right)$ 的性状来判断级数 $F(s)=\sum f(n)n^{-s}$ 的解析特性．实际上，由 $F(s)$

的解析特性来判断和估计 $f(n)$ 或者 $A(N)$ 的阶，则是解析数论的更重要的课题．解析数论在这一方向上的许多方法和结果也可推广到代数数域中去．例如我们在第六章中要将通常的素数定理推广成任意代数数域中的素理想定理．但是本书在这方面不准备作深入的探讨．

习　题

1． 求证：

(a) $\sum_{n=1}^{\infty}\mu(n)^2n^{-s}=\zeta(s)/\zeta(2s)$；

(b) $\sum_{n=1}^{\infty}2^{\omega(n)}n^{-s}=\zeta(s)^2/\zeta(2s)$；

(c) 对于 $n=p_1^{a_1}\cdots p_r^{a_r}$，定义 $\lambda(n)=(-1)^{a_1+\cdots+a_r}$，求证 $\sum_{n=1}^{\infty}\lambda(n)n^{-s}=\zeta(2s)/\zeta(s)$．

2． 求证：

(a) $\sum_{d\mid n}\lambda(d)=\begin{cases}1, & \text{若 } n \text{ 为完全平方;}\\ 0, & \text{否则;}\end{cases}$

(b) $\varphi(n)/n=\sum_{d\mid n}\mu(d)/d,\ n/\varphi(n)=\sum_{d\mid n}\mu^2(d)/\varphi(d)$；

(c) $\{\lambda(n)\}$ 对于卷积运算的逆元素为 $\{|\mu(n)|\}$；

(d) $\Lambda(n)=-\sum_{d\mid n}\mu(d)\log d$，其中 $\Lambda(n)$ 为 Mangoldt 函数．

3． 如果 f 和 g 均为积性数论函数，求证 $f*g$ 也是积性数论函数．对于完全积性函数这一命题是否成立？

4． 如果 f 为积性数论函数，则 $\sum_{d\mid n}\mu(d)f(d)=\prod_{p\mid n}(1-f(p))$．

5． 令 $\zeta_n=e^{2\pi i/n}$，求证 $\mu(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}\zeta_n^k$．

6． 假设 R 是任意带 1 交换环，f：$\mathbb{Q}\to R$．令

$$F(n)=\sum_{k=1}^{n}f(k/n),\quad \widetilde{F}(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}f(k/n).$$

求证：$\{\widetilde{F}(n)\}=\{F(n)\}*\{\mu(n)\}$．

7． 设 σ_0 和 σ_1 分别为 D-级数 $\sum_{n=1}^{\infty}a_nn^{-s}(a_n\in\mathbb{C})$ 的收敛横坐标和绝对收敛

横坐标. 求证 $\sigma_0 \leqslant \sigma_1 \leqslant \sigma_0+1$, 并给出 $\sigma_1=\sigma_0$ 和 $\sigma_1=\sigma_0+1$ 的两个 D-级数的例子.

8. (唯一性定理)如果 $A(s)=\sum_{n=1}^{\infty} a_n n^{-s}$ 和 $B(s)=\sum_{n=1}^{\infty} b_n n^{-s}$ 在复平面的某个右半平面内定义出同一个复变函数, 求证 $a_n=b_n(n=1, 2, \cdots)$.

9. 求证当 $\mathrm{Re}(s)>1$ 时, $-\zeta'(s)/\zeta(s)=\sum_{n=1}^{\infty} \Lambda(n) n^{-s}$, 其中 $\Lambda(n)$ 是 Mangold 函数.

§2 Riemann zeta 函数 $\zeta(s)$ 和 Dirichlet L 函数 $L(s, \chi)$

2.1 $\zeta(s)$ 的函数方程, Riemann 猜想

我们在上一节中看到, 许多数论函数的 Dirichlet 级数都可用 Riemann zeta 函数 $\zeta(s)$ 表示出来, 所以有必要对于 $\zeta(s)$ 的解析性质作更深入的研究. 我们已经把 $\zeta(s)$ 解析延拓到半平面 $\mathrm{Re}(s)>0$ 之中, 在这个半平面中 $\zeta(s)$ 只有一个奇点 $s=1$, 并且是留数为 1 的单极点. Riemann 另一个杰出贡献是: 他建立了 $\zeta(s)$ 的函数方程, 从而将 $\zeta(s)$ 解析延拓到整个复平面上.

定理 4 $\zeta(s)$ 可以解析延拓到整个复平面上, 并且满足下面的函数方程

$$\pi^{-s/2}\Gamma(s/2)\zeta(s)=\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s),$$

其中 $\Gamma(s)$ 是 Gamma 函数.

在证明定理 4 之前, 我们概要地叙述一下 Gamma 函数 $\Gamma(s)$ 的一些基本事实, 然后介绍证明定理 4 的基本工具——Poisson 求和公式, 最后给出定理 4 的证明和一些推论.

(1) Gamma 函数 $\Gamma(s)$

Gamma 函数的 Euler 定义是 $\Gamma(s)=\int_0^{\infty} x^{s-1}e^{-x}\mathrm{d}x$. 右边积分在 $\mathrm{Re}(s)>0$ 时收敛. 分部积分给出 $\Gamma(s+1)=s\Gamma(s)$. 由此可将 $\Gamma(s)$ 解析延拓到整个复平面上, 并且显然有 $\Gamma(n+1)=n!$ 注意

$$\frac{1}{\Gamma(s)}=\frac{s}{\Gamma(s+1)}=\frac{s(s+1)\cdots(s+n)}{\Gamma(s+n+1)}$$
$$=\frac{\Gamma(n+1)}{\Gamma(s+n+1)}s(1+s/1)(1+s/2)\cdots(1+s/n).$$

不幸的是，无穷乘积 $\prod_{n=1}^{\infty}(1+s/n)$ 发散. 补救办法是加上"收敛因子"$e^{-s/n}$，于是 $\prod_{n=1}^{\infty}(1+s/n)e^{-s/n}$ 收敛. 由 $\sum_{k=1}^{n}\frac{1}{k}=\log n+\gamma+O\left(\frac{1}{n}\right)$ (γ 叫作是 Eulor 常数)和渐近公式 $\Gamma(n+s)\sim n^{s-1}\left(\frac{n}{e}\right)^{n}\sqrt{2\pi n}$，可以推导出 $1/\Gamma(s)$ 的 Weierstrass 无穷乘积展开式:

$$1/\Gamma(s)=se^{\gamma s}\prod_{n=1}^{\infty}(1+s/n)e^{-s/n}.$$

从而 $\frac{1}{\Gamma(s)}$ 为整函数，零点为 $s=0,\ -1,\ -2,\ \cdots$，并且均是单零点. 于是 $\Gamma(s)$ 在整个复平面上只有奇点 $s=0,\ -1,\ -2,\ \cdots$，并且均是单极点. 且留数为 $\operatorname{res}_{s=-n}\Gamma(s)=(-1)^{n}/n!$. 由 $1/\Gamma(s)$ 的无穷乘积展开式还可得到

$$1/\Gamma(s)\Gamma(-s)=s^{2}\prod_{n=1}^{\infty}(1-s^{2}/n^{2})=-s\frac{\sin\pi s}{\pi},$$

即 $\Gamma(s)\Gamma(1-s)=\pi/\sin\pi s$. 由此可知 $\Gamma(1/2)=\sqrt{\pi}$.

(2) Poisson 求和公式

设 $g(x)$ 是周期为 1 的实变函数. 在适当的条件下(见后)，它有 Fourier 展开:

$$g(x)=\sum_{n=-\infty}^{\infty}a_{n}e^{2\pi inx},\quad a_{n}=\int_{0}^{1}g(x)e^{-2\pi inx}\,dx.$$

现在设 $f(x)$ 是 $(-\infty,\ \infty)$ 上的连续函数，而 $g(x)=\sum_{n=-\infty}^{\infty}f(n+x)$. 如果 $g(x)$ 有意义的话，$g(x)$ 显然是周期为 1 的实变函数. 这时，如果 $g(x)$ 可作 Fourier 展开，那末其 Fourier 系数为

$$a_{k}=\int_{0}^{1}\left(\sum_{n=-\infty}^{\infty}f(x+n)\right)e^{-2\pi ikx}\,dx=\sum_{n=-\infty}^{\infty}\int_{0}^{1}f(x+n)e^{-2\pi ikx}\,dx$$
$$=\sum_{n=-\infty}^{\infty}\int_{n}^{n+1}f(x)e^{-2\pi ikx}\,dx=\int_{-\infty}^{\infty}f(x)e^{-2\pi ikx}\,dx.$$

取 $x=0$ 即得到

$$\sum_{n=-\infty}^{\infty} f(n)=g(0)=\sum_{n=-\infty}^{\infty} a_n,$$

以上推导中我们随意地写上 $\sum_{-\infty}^{\infty}\int_{-\infty}^{\infty}$ 以及交换 Σ 和 $\int$ 的次序. 作为微积分的很好练习，请读者自行验证，在下述引理诸条件(a)～(d)均成立的时候，上面的推导是合理的. 这就使我们得到

引理 4(Poisson 求和公式) 假设 $f(x)$ 为实变函数，并且

(a) $f(x)$ 在 $(-\infty, \infty)$ 上连续;

(b) $\sum_{n=-\infty}^{\infty} f(x+n)$ 在每个有限区间 $a\leqslant x\leqslant b$ 上均一致收敛;

(c) 积分 $\int_{-\infty}^{\infty} |f(x)|\mathrm{d}x$ 收敛;

(d) 级数 $\sum_{k=-\infty}^{\infty}|a_k|$ 收敛，其中 $a_k=\int_{-\infty}^{\infty} f(x)e^{-2\pi ikx}\mathrm{d}x$, 则 $\sum_{n=-\infty}^{\infty} f(n)=\sum_{n=-\infty}^{\infty} a_n$. ▌

(3) 定理 4 的证明

当 $\mathrm{Re}(s)>1$, $t>0$ 时,

$$\begin{aligned}\pi^{-s/2}\zeta(s)\Gamma(s/2)&=\int_0^{\infty}\pi^{-s/2}\sum_{n=1}^{\infty} n^{-s}t^{s/2-1}e^{-t}\,\mathrm{d}t\quad (t\mapsto \pi n^2 t)\\&=\int_0^{\infty} t^{s/2-1}\left(\sum_{n=1}^{\infty}e^{-\pi n^2 t}\right)\mathrm{d}t=\int_0^1+\int_1^{\infty}\\&=\int_1^{\infty}x^{s/2-1}w(x)\,\mathrm{d}x+\int_1^{\infty}x^{-s/2-1}w(x^{-1})\,\mathrm{d}x,\quad (*)\end{aligned}$$

其中 $w(x)=\sum_{n=1}^{\infty}e^{-n^2\pi x}$. 令 $\theta(x)=\sum_{n=-\infty}^{\infty}e^{-n^2\pi x}=1+2w(x)$. 在 Poisson 公式中取 $f(t)=e^{-t^2\pi x}$, 则 $a_n=\int_{-\infty}^{\infty}f(t)e^{-2\pi int}\,\mathrm{d}t=\frac{1}{\sqrt{x}}e^{-\pi n^2/x}$. 不难验证引理 4 中诸条件均成立(原因是当 $|t|\to\infty$ 时 $f(t)$ 下降很快). 于是

$$\theta(x)=\sum_{n=-\infty}^{\infty}f(n)=\frac{1}{\sqrt{x}}\sum_{n=-\infty}^{\infty} e^{-\pi n^2/x}=\frac{1}{\sqrt{x}}\theta(1/x),$$

从而 $w(1/x)=-1/2+\sqrt{x}/2+\sqrt{x}\,w(x)$. 将此代入(*)式得到

$$\pi^{-s/2}\Gamma(s/2)\zeta(s)=-1/s-1/(1-s)+\int_1^\infty x^{s/2-1}w(x)\mathrm{d}x$$

$$+\int_1^\infty x^{\frac{1-s}{2}-1}w(x)\mathrm{d}x.$$

但是上式右边两个积分对于任何 s 值均有意义，所以通过上式将 $\zeta(s)$ 解析延拓到整个复平面上，并且如果将 s 改成 $1-s$，上式右边不变，从而

$$\pi^{-s/2}\Gamma(s/2)\zeta(s)=\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \qquad \blacksquare$$

系 (a) $\zeta(s)$ 在整个复平面上只有一个奇点 $s=1$，并且是留数为 1 的单极点.

(b) $s=-2, -4, -6, \cdots$ 是 $\zeta(s)$ 的单零点（称作是 $\zeta(s)$ 的平凡零点）. 而 $\zeta(s)$ 的其他零点均在区域 $0<\mathrm{Re}(s)<1$ 之内，并且这些零点对于垂直线 $\mathrm{Re}(s)=1/2$ 是对称的.

证明 当 $\mathrm{Re}(s)>1$ 时，$\zeta(s)$ 有收敛的无穷乘积展开式，从而 $\zeta(s)$ 无零点也无奇点. 当 $\mathrm{Re}(s)<0$ 时

$$\zeta(s)=\pi^{s-1/2}\zeta(1-s)\Gamma(1-s/2)/\Gamma(s/2), \qquad (*)$$

由于 $\mathrm{Re}(1-s)>1$，从而这时 $\zeta(s)$ 的奇点与零点只与 Gamma 函数有关. 由于 $\Gamma(s)$ 无零点，而只有极点 $0, -1, -2, \cdots$，并且均是单极点，$\operatorname*{res}_{s=-n}\Gamma(s)=(-1)^n/n!$. 从而由 $(*)$ 式即知 $\zeta(s)$ 在 $\mathrm{Re}(s)<0$ 中没有极点，而零点只有 $s=-2,-4,-6,\cdots$，并且均是单零点 $\left(\text{注意在 } s=0 \text{ 处，} \zeta(0)=\lim\limits_{s\to0}\dfrac{\pi^{-1/2}\zeta(1-s)\Gamma(1/2)}{\Gamma(s/2)}=\lim\limits_{s\to0}\dfrac{s/2}{(1-s)-1}=-1/2\neq0\right)$. 在 $0\leqslant\mathrm{Re}(s)\leqslant1$ 中，我们已经证明了 $\zeta(s)$ 只有一个极点 $s=1$. 由 $(*)$ 式即知在直线 $\mathrm{Re}(s)=0$ 上 $\zeta(s)$ 无奇点. 于是在整个复平面上只有一个（单）奇点 $s=1$. 最后，下面引理 5 表明 $\zeta(s)$ 在直线 $s=1+it$ 上无零点，从而由 $(*)$ 式表明 $\zeta(s)$ 在直线 $s=it$ 上也无零点，这就表明 $\zeta(s)$ 的非平凡零点均在区域 $0<\mathrm{Re}(s)<1$ 中. 并且若 s_0 是 $\zeta(s)$ 在此区域中的零点，则由 $(*)$ 式可知 $1-s_0$ 也是 $\zeta(s)$ 在此区域中的零点，从而非平凡零点关于直线

$\mathrm{Re}(s)=1/2$ 是对称的. ▌

注记 著名的 **Riemann** 猜想是说: $\zeta(s)$的非平凡零点均在直线 $\mathrm{Re}(s)=\frac{1}{2}$ 之上. 人们已经验证了, 按照零点绝对值的大小, 前 1.5×10^8 个非平凡零点均在 $\mathrm{Re}(s)=1/2$ 直线上. 例如其中前 8 个零点为: $\frac{1}{2}\pm i(14.134725\cdots)$, $\frac{1}{2}\pm i(21.022040\cdots)$, $\frac{1}{2}\pm i(25.010856\cdots)$和 $\frac{1}{2}\pm i(30.424878\cdots)$, 但是 Riemann 猜想至今未被证明或推翻.

引理 5 对于任意 $t\in\mathbb{R}$, $\zeta(1+it)\neq0$.

证明 令 $s=\sigma+it$. 当 $\sigma>1$ 时 $\zeta(s)=\prod\limits_p(1-p^{-s})^{-1}$, 从而

$$\log\zeta(s)=-\sum_p\log(1-p^{-s})=\sum_p\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}.$$

因此若令 $\exp(\alpha)=e^{\alpha}$, 则 $\zeta(s)=\exp\left(\sum\limits_p\sum\limits_{m=1}^{\infty}e^{-imt\log p}/mp^{m\sigma}\right)$, 从而 $|\zeta(s)|=\exp\left\{\sum\limits_p\sum\limits_{m=1}^{\infty}\cos(mt\log p)/mp^{m\sigma}\right\}$, 于是

$$\zeta^3(\sigma)|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|=\exp\left\{\sum_p\sum_{m=1}^{\infty}A_m/mp^{m\sigma}\right\},$$

其中

$$\begin{aligned}A_m&=3+4\cos(mt\log p)+\cos(2mt\log p)\\&=2\{\cos(mt\log p)+1\}^2\geqslant0.\end{aligned}$$

从而 $\zeta^3(\sigma)|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|\geqslant1$(当 $\sigma>1$ 时), 或者写成:

$$((\sigma-1)\zeta(\sigma))^3\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4|\zeta(\sigma+2it)|\geqslant\frac{1}{\sigma-1}\ (\sigma>1\text{ 时}).$$

我们已经知道 $s=1$ 是 $\zeta(s)$ 的奇点; 另一方面, 如果 $1+it(t\neq0)$ 为 $\zeta(s)$ 的零点, 由定理 4 的系可知当 $\sigma\to1$ 时, 上式左边为常数, 而右边 $\to\infty$, 这就导致矛盾. ▌

2.2 有限 Abel 群的特征

定义 3 设 G 是有限 Abel 群(运算记为乘法), 从 G 到乘法群 $\mathbb{C}^*=\mathbb{C}-\{0\}$的每个同态 χ: $G\to\mathbb{C}^*$ 均叫作是群 G 的特征.

如果 $|G|=n$，则对于每个 $g\in G$，$\chi(g)^n=\chi(g^n)=\chi(1_G)=1$。因此特征 χ 的取值均是 n 次单位根.

例 1 $\chi\equiv 1$ 显然是 G 的特征，称作是 G 的主特征，记为 χ_0。

例 2 设 $C_n=\langle a|a^n=1\rangle$ 是 n 阶循环群，χ 为 C_n 的特征. 由上述可知 $\chi(a)=\omega^t$，$\omega=e^{2\pi i/n}$，$0\leqslant t\leqslant n-1$. 并且 χ 由它在 a 处的取值所完全决定：$\chi(a^j)=\omega^{tj}(0\leqslant j\leqslant n-1)$. 这个特征记为 χ_t，于是 $\{\chi_0, \chi_1, \cdots, \chi_{n-1}\}$ 就是 C_n 的全部 n 个不同的特征.

以 $\hat{G}$ 表示有限 Abel 群 G 的全部特征所构成的集合. 对于 χ, $\chi'\in\hat{G}$，定义特征的乘法 $\chi\chi'$ 为 $\chi\chi'(g)=\chi(g)\chi'(g)\ (g\in G)$，易知 $\chi\chi'$ 也是群 G 的特征，并且 $\hat{G}$ 由此形成 Abel 群，叫作是 G 的特征群. $\hat{G}$ 中单位元素即是主特征 χ_0. 若 χ^{-1} 表示特征 χ 的逆，则 $\chi^{-1}(g)=\chi(g)^{-1}=\overline{\chi(g)}$（注意 $\chi(g)$ 是单位根），即 $\chi^{-1}(g)$ 是 $\chi(g)$ 的复共轭. 因此也将 χ^{-1} 表示成 $\bar{\chi}$，称作是 χ 的共轭特征.

定理 5 设 G 为有限 Abel 群. 则其特征群 $\hat{G}$ 与 G 正则同构.

证明 我们知道，每个有限 Abel 群 G 均是有限个循环群的直积：$G=C_{n_1}\times C_{n_2}\times\cdots\times C_{n_r}$，$C_{n_t}=\langle a_t|a_t^{n_t}=1\rangle$ 为 G 的 n_t 阶循环子群 $(1\leqslant t\leqslant r)$. 设 $\chi\in\hat{G}$，χ 在每个子群 C_{n_t} 上的限制显然为 C_{n_t} 的特征，从而由前例 2 知 $\chi(a_t)=\zeta_{n_t}^{j_t}(0\leqslant j_t\leqslant n_t-1)$. 由于 G 中元素唯一地表示成 $a_1^{i_1}\cdots a_r^{i_r}(0\leqslant i_t\leqslant n_t-1,\ 1\leqslant t\leqslant r)$，从而

$$\chi(a_1^{i_1}\cdots a_r^{i_r})=\chi(a_1)^{i_1}\cdots\chi(a_r)^{i_r}=\zeta_{n_1}^{i_1j_1}\cdots\zeta_{n_r}^{i_rj_r}$$

对于每组 $(j_1, \cdots, j_r)$. 易知上式定义的函数均是 G 的特征. 将它表示成 $\chi_{j_1,\cdots,j_r}$，则 $\{\chi_{j_1,\cdots,j_r}|j_t\in\mathbb{Z},\ 1\leqslant t\leqslant r\}$ 就是 G 的全部可能的特征，易知

$$\chi_{j_1,\cdots,j_r}=\chi_{j'_1,\cdots,j'_r}\Leftrightarrow j_t\equiv j'_t\ (\bmod n_t)\quad(1\leqslant t\leqslant r).$$

从而若将 j_t 看成是 $\mathbb{Z}/n_t\mathbb{Z}$ 中元素，则

$$\{\chi_{j_1,\cdots,j_r}|j_t\in\mathbb{Z}/n_t\mathbb{Z},\ 1\leqslant t\leqslant r\}$$
$$=\{\chi_{j_1,\cdots,j_r}|0\leqslant j_t\leqslant n_t-1,\ 1\leqslant t\leqslant r\}$$

就是 G 的全部特征，并且两两不同. 又易证

$$\chi_{j_1,\cdots,j_r}\cdot\chi_{j'_1,\cdots,j'_r}=\chi_{j_1+j'_1,\cdots,j_r+j'_r}.$$

从而映射 $\psi:\ \hat{G}\to G,\ \chi_{j_1,\cdots,j_r}\mapsto a_1^{j_1}\cdots a_r^{j_r}$

是群 $\hat{G}(\cong\mathbb{Z}/n_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/n_r\mathbb{Z})$ 与群 $G=C_{n_1}\times\cdots\times C_{n_r}$ 的同构. ∎

例 1 5 阶循环群 $C_5=\langle a\,|\,a^5=1\rangle$的特征群为

$$\hat{C}_5=\langle\chi^i\,|\,0\leqslant i\leqslant 5\rangle,$$

其中 $\chi(a)=\omega,\ \omega=e^{2\pi i/5}$. 从而全部特征取值如下表所示:

	1	a	a^2	a^3	a^4
$\chi_0=\chi^0$	1	1	1	1	1
χ	1	ω	ω^2	ω^3	ω^4
χ^2	1	ω^2	ω^4	ω	ω^3
χ^3	1	ω^3	ω^1	ω^4	ω^2
χ^4	1	ω^4	ω^3	ω^2	ω

例 2 (2.2)型 Abel 群 $C_2\times C_2=\langle a,\ b\,|\,a^2=b^2=1,\ ab=ba\rangle$ 的特征群为 $\hat{G}=\{\chi_0,\ \chi_1,\ \chi_2,\ \chi_1\chi_2\}$,其值为

	1	a	b	ab
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
$\chi_1\chi_2$	1	-1	-1	1

定理 6(正交关系) 设 G 为 n 阶 Abel 群,则

(a) $\displaystyle\sum_{g\in G}\chi(g)=\begin{cases}n, & \text{如果 } \chi=\chi_0;\\ 0, & \text{否则.}\end{cases}$

(b) $\displaystyle\sum_{\chi\in}\chi(g)=\begin{cases}n, & \text{如果 } g=1_G;\\ 0, & \text{否则.}\end{cases}$

证明 (a) 显然 $\sum\limits_{g\in G}\chi_0(g)=\sum\limits_{g\in G}1=|G|=n$. 如果 $\chi=\chi_0$, 则存在 $b\in G$ 使得 $\chi(b)\neq1$,于是

$$\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(bg)=\sum_{g\in G}\chi(b)\chi(g)=\chi(b)\sum_{g\in G}\chi(g).$$

但是 $\chi(b)\neq1$, 从而必然 $\sum\limits_{g\in G}\chi(g)=0$.

(b) 显然 $\sum\limits_{\chi\in\hat{G}}\chi(1)=\sum\limits_{\chi\in\hat{G}}1=|\hat{G}|=|G|=n$. 如果 $g\neq1$, 令 $G'=\langle g\rangle$为元素 g 生成的 G 之子群, 则 $|G'|>1$, 于是 $|G/G'|<n$.

令 $H=\{\chi\in\hat{G}\mid\chi(g)=1\}$，则对于每个 $\chi\in H$，同态 $\chi: G\to\mathbb{C}^*$ 的核 $\ker\chi\supseteq G'$，从而自然诱导出商群 G/G' 的特征 $\tilde{\chi}: G/G'\to\mathbb{C}^*$．并且对于 H 中两个不同的特征 χ 和 χ'，$\tilde{\chi}$ 与 $\tilde{\chi}'$ 也不相同．但是 G/G' 的特征共有 $|G/G'|$ 个，这就表明

$$|H|\leqslant|(G/G')^\wedge|=|G'/G|<n=|G|=|\hat{G}|.$$

于是 $H\subsetneqq\hat{G}$，从而存在 $\psi\in\hat{G}$，使得 $\psi(g)\neq1$，于是

$$\sum_{\chi\in\hat{G}}\chi(g)=\sum_{\chi\in\hat{G}}\psi\chi(g)=\sum_{\chi\in\hat{G}}\psi(g)\chi(g)=\psi(g)\sum_{\chi\in\hat{G}}\chi(g).$$

由于 $\chi(g)\neq1$，因此必然 $\sum\limits_{\chi\in\hat{G}}\chi(g)=0$． ▌

定义 4 加法群 $\mathbb{Z}/m\mathbb{Z}$ 的每个特征 λ 叫作是**模 m 加法特征**．由于 $\mathbb{Z}/m\mathbb{Z}$ 是 m 阶循环群，从而它的特征群也是 m 阶循环群．其生成元可取为 $\lambda: \mathbb{Z}/m\mathbb{Z}\to\mathbb{C}^*$，$\lambda(1)=\zeta_m$．从而模 m 加法特征群为 $\{\lambda^a\mid0\leqslant a\leqslant m-1\}$，其中 $\lambda^a(n)=e^{2\pi ina/m}=\zeta_m^{an}$ $(\bar{n}\in\mathbb{Z}/m\mathbb{Z})$．

乘法群 $(\mathbb{Z}/m\mathbb{Z})^*$ 的每个特征叫作是模 m 乘法特征，通常也称作是**模 m 的 Dirichlet 特征**，简称作**模 m 的D–特征**．从定理 5 的证明可知，为了决定模 m 的全部 D–特征，我们只需弄清有限 Abel 群 $(\mathbb{Z}/m\mathbb{Z})^*$ 的结构．这是初等数论的内容．详言之，设 $m=p_1^{a_1}\cdots p_r^{a_r}$ 为 m 的素因子分解式，则由中国剩余定理知道

$$(\mathbb{Z}/m\mathbb{Z})^*\cong(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^*\times\cdots\times(\mathbb{Z}/p_r^{a_r}\mathbb{Z})^*.$$

而 $(\mathbb{Z}/p^n\mathbb{Z})^*$ 的结构为：

(a) 当 $p\geqslant3$，$n\geqslant1$ 时 $(\mathbb{Z}/p^n\mathbb{Z})^*$ 是 $\varphi(p^n)$ 阶循环群，其生成元 g 可取为模 p^n 的任何一个原根．

(b) $(\mathbb{Z}/2\mathbb{Z})^*=\{1\}$，$(\mathbb{Z}/4\mathbb{Z})^*=\{\pm1\}$ (2 阶循环群)，而当 $n\geqslant3$ 时，$(\mathbb{Z}/2^n\mathbb{Z})^*=\langle-1\rangle\times\langle5\rangle$，其中 -1 和 5 分别生成 $(\mathbb{Z}/2^n\mathbb{Z})^*$ 的 2 阶和 2^{n-2} 阶循环子群．

由此完全决定了乘法群 $(\mathbb{Z}/m\mathbb{Z})^*$ 的结构，然后不难写出全部 $\varphi(m)$ 个模 m 的D–特征．

例 1 $(\mathbb{Z}/4\mathbb{Z})^*=\{\pm1\}$，从而模 4 有两个 D–特征：$\chi_0$ 和 χ_1．

	1	−1(=3)
χ_0	1	1
χ_1	1	−1

例 2 $(\mathbb{Z}/8\mathbb{Z})^*=\langle-1\rangle\times\langle+5\rangle$，而 -1 和 5 均生成 2 阶循环群。从而模 8 有四个 D-特征：χ_0，χ_1，χ_2，$\chi_3=\chi_1\chi_2$

	1	−1=7	5	−5=3
χ_0	1	1	1	1
χ_1	1	−1	1	−1
χ_2	1	1	−1	−1
$\chi_1\chi_2=\chi_3$	1	−1	−1	1

例 3 $(\mathbb{Z}/5\mathbb{Z})^*=\langle 3\rangle$，即是由模 5 的原根 3 生成的 4 阶循环群。从而模 5 的四个 D-特征为 χ_0，χ，χ^2 和 χ^3，其中 $\chi(3)=i=\sqrt{-1}$。

	1	3	$3^2=4$	$3^3=2$
χ_0	1	1	1	1
χ	1	i	−1	$-i$
χ^2	1	−1	1	−1
$\overline{\chi}_0=\chi^3$	1	$-i$	−1	i

定义 5 设 χ 为模 m 的 D-特征，由于 $\chi(-1)^2=\chi(1)=1$，从而 $\chi(-1)=\pm1$。如果 $\chi(-1)=1$，称 χ 为偶特征；如果 $\chi(-1)=-1$，称 χ 为奇特征。

引理 6 设 χ 是模 m 的 D-特征，$d|m$，则下列三个条件彼此等价。

(a) 存在模 d 的 D-特征 χ'，使得 $(m, a)=1$（从而 $(d, a)=1$）时，$\chi(a)=\chi'(a)$；

(b) $(a, m)=1$，$a\equiv1(\operatorname{mod} d)\Rightarrow\chi(a)=1$；

(c) $(a, m)=(a', m)=1$，$a\equiv a'(\operatorname{mod} d)\Rightarrow\chi(a)=\chi(a')$。

证明 (a)⇒(b)⇒(c) 是显然的。剩下只需再证 (c)⇒(a)。我们如下定义一个函数 χ'：若 $(a, d)=1$，则存在 $a'\in\mathbb{Z}$，使得 $a'\equiv a(\operatorname{mod} d)$ 并且 $(a', m)=1$（令 $q=\prod\limits_{\substack{p|m\\p\nmid a}}p$，取 $a'=a+qd$ 即为所求）。

如果条件(c)成立，则我们可以定义函数 $\chi'(a)=\chi(a')$. 易知这是模 d 的 D-特征，并且当 $(a, m)=1$ 时，$\chi'(a)=\chi(a')=\chi(a)$. ▌

定义 如果引理 6 中的条件成立，并且 d 是 m 的真因子(即 $d|m$, $1\leqslant d<m$)，则称 χ 是模 m 的**非本原 D-特征**. 因为 χ 是由 χ' 诱导出来的，而 χ' 有比 χ 小的模，否则，如果不存在 m 的真因子 d 使得引理 6 中的条件成立，便称 χ 是模 m 的**本原 D-特征**. 而满足引理 6 中条件的最小正数 d 称作是特征 χ 的**导子** (Conductor, 德文 Führer)，记为 $\mathrm{cond}(\chi)$.

引理 7 设 χ 为模 m 的 D-特征，$\mathrm{cond}(\chi)=d$，则 χ 是由模 d 的某个本原 D-特征诱导出来的.

证明 根据定义可知 χ 可由模 d 的某个 D-特征 χ' 诱导出来. 即 $(a, m)=1$ 时，$\chi(a)=\chi'(a)$. 如果 χ' 不是模 d 本原特征，则存在 d 的真因子 d' 和模 d' 的 D-特征 χ''，使得 $(a, d)=1$ 时 $\chi'(a)=\chi''(a)$. 于是当 $(a, m)=1$(从而 $(a, d)=1$)时，$\chi(a)=\chi''(a)$. 即 χ 也是由 χ'' 诱导出来的. 但是 χ'' 具有模 $d'<d$，这就与 $\mathrm{cond}(\chi)=d$ 相矛盾，从而 χ' 必为模 d 的本原 D-特征. ▌

比如：前面给出模 8 的四个 D-特征中，χ_2 和 χ_3 是模 8 的本原特征：$\mathrm{cond}(\chi_2)=\mathrm{cond}(\chi_3)=8$，而 χ_1 是由模 4 本原特征 "$\chi(1)=1$, $\chi(-1)=-1$"诱导出来的，从而 $\mathrm{cond}(\chi_1)=4$. 最后，主特征 χ_0 的导子必为 1.

最后我们来计算将模 m 加法特征与乘法特征放在一起的一个和式——Gauss 和它在数论中起重要的作用. 设 λ 和 χ 分别是模 m 的加法特征与 D-特征. 为方便起见，当 $(m, a)>1$ 时，我们规定 $\chi(a)=0$.

定义 6 $G(\lambda, \chi)=\sum\limits_{n=0}^{m-1}\lambda(n)\chi(n)$ 叫作**模 m 的 Gauss 和**. 由于模 m 的加法特征均有形式 $\lambda_k(n)=e^{2\pi ikn/m}$ $(0\leqslant k\leqslant m-1)$，从而 Gauss 和也可写成

$$G(k, \chi)=\sum_{m=0}^{m-1}\chi(n)e^{2\pi ikn/m}.$$

注记 我们在第三章中计算过和式 $G_p(r)=\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e^{2\pi irn/p}$，这是一个模 p 的 Gauss 和，因为$\left(\frac{n}{p}\right)=\chi(n)$为模 p 的 D-特征。

定理 7 (a) 若$(k, m)=1$，则 $G(k, \chi)=\overline{\chi}(k)G(1, \chi)$.

(b) 若 χ 为模 m 的本原 D-特征，则$|G(1, \chi)|=\sqrt{m}$. 并且当$(k, m)>1$ 时，$G(k, \chi)=0$.

证明 (a) 如果$(k, m)=1$，则

$$G(k, \chi)=\sum_{n=0}^{m-1}\chi(n)e^{\frac{2\pi ikn}{m}}=\sum_{n=0}^{m-1}\overline{\chi}(k)\chi(nk)e^{2\pi ikn/m}$$

$$=\overline{\chi}(k)\sum_{n=0}^{m-1}\chi(n)e^{2\pi in/m}=\overline{\chi}(k)G(1, \chi).$$

(b) 如果$(k, m)=d>1$，令 $k=k'd$, $m=m'd$，则 $m'<m$. 由于 χ 是模 m 本原 D-特征，由引理 6 可知有 $r\in\mathbb{Z}$, $r\equiv1(\bmod m')$, $(r, m)=1$，而 $\chi(r)\neq1$. 于是

$$G(k, \chi)=\sum_{n=0}^{m-1}\chi(n)e^{2\pi ink'/m'}=\sum_{\lambda=0}^{m'-1}e^{2\pi ik'\lambda/m'}\sum_{\substack{n=0\\ n\equiv\lambda(\bmod m')}}^{m-1}\chi(n)$$

$$=\sum_{\lambda=0}^{m'-1}e^{2\pi ik'\lambda/m'}\sum_{\substack{n=0\\ n\equiv\lambda(\bmod m')}}^{m-1}\chi(nr)$$

$$=\chi(r)\sum_{\lambda=0}^{m'-1}e^{2\pi ik'\lambda/m'}\sum_{\substack{n=0\\ n\equiv\lambda(\bmod m')}}^{m-1}\chi(n)=\chi(r)G(k, \chi).$$

但是 $\chi(r)\neq1$，从而 $G(k, \chi)=0$. 另一方面，

$$|G(1, \chi)|^2=G(1, \chi)\overline{G(1, \chi)}=G(1, \chi)\sum_{n=0}^{m-1}\overline{\chi}(n)e^{-2\pi in/m}$$

$$=\sum_{n=0}^{m-1}G(n, \chi)e^{-2\pi in/m}=\sum_{n, n'=0}^{m-1}\chi(n')e^{(2\pi in'n-2\pi in)/m}$$

$$=\sum_{n'=0}^{m-1}\chi(n')\sum_{n=0}^{m-1}e^{2\pi in(n'-1)/m}=m\chi(1)=m.$$

从而$|G(1, \chi)|=\sqrt{m}$. ∎

2.3 Dirichlet L 函数

设 χ 为模 m 的 D-特征. 当$(m, n)>1$ 时规定 $\chi(n)=0$. 如下定义一个 D-级数

$$L(s, \chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}.$$

称作是 Dirichlet L 函数. 当 $\chi\neq\chi_0$ 时由于$\{\chi(n)\mid n=1, 2, \cdots\}$的部分和是发散并且有界的(习题 12). 从而 $L(s, \chi)$的收敛横坐标为 $\sigma_0=0$, 而绝对收敛横坐标显然为 $\sigma_1=1$. 于是它在半平面 $\mathrm{Re}(s)>0$ 内定义了一个正则函数. 由于特征 χ 是完全积性的, 于是当 $\mathrm{Re}(s)>\sigma_1=1$ 时有 Euler 乘积展开:

$$L(s, \chi)=\prod_{p}(1-\chi(p)p^{-s})^{-1}=\prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1}$$

$$(\mathrm{Re}(s)>1).$$

如果 cond $\chi=m'|m$, 并且 χ 是由模 m' 的本原 D-特征 χ' 诱导出来的(引理 6), 则

$$\begin{aligned}L(s, \chi)&=\prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1}=\prod_{p\nmid m}(1-\chi'(p)p^{-s})^{-1}\\&=\prod_{p}(1-\chi'(p)p^{-s})^{-1}\cdot\prod_{p\mid m}(1-\chi'(p)p^{-s})\\&=L(s, \chi')\cdot\prod_{p\mid m}(1-\chi'(p)p^{-s}).\end{aligned}$$

于是 $L(s, \chi)$和 $L(s, \chi')$只相差一个有限乘积. 所以只需研究对本原 D-特征的 L 函数即可. 特别对于模 m 的主特征 χ_0, 我们有

$$L(s, \chi_0)=\zeta(s)\prod_{p\mid m}(1-p^{-s}).$$

与 $\zeta(s)$一样, 为了将 $L(s, \chi)$延拓到整个复平面上, 需要函数方程.

定理 8 设 χ 为模 N 的本原 D-特征. 令

$$\delta(\chi)=\delta=\begin{cases}0, & 若\ \chi(-1)=1;\\1, & 若\ \chi(-1)=-1,\end{cases}$$

$$\xi(s, \chi)=\left(\frac{N}{\pi}\right)^{s/2}\Gamma\left(\frac{s+\delta}{2}\right)L(s, \chi),$$

则 $L(s, \chi)$可以解析延拓到整个复平面上并且满足如下的函数方程

$$\xi(s, \chi)=\frac{G(1, \chi)}{i^{\delta}\sqrt{N}}\xi(1-s, \bar{\chi}).$$

证明 基本工具仍是 Poisson 求和公式. 我们分两种情况考

虑.

(a) χ 为偶特征. 即 $\chi(-1)=1$, 此时 $\delta=0$. 由于

$$\left(\frac{N}{\pi}\right)^{s/2}\Gamma(s/2)n^{-s}=\int_0^{\infty}e^{-n^2\pi x/N}x^{s/2-1}\,dx,$$

从而当 $\mathrm{Re}(s)=\sigma>1$ 时,

$$\begin{aligned}\xi(s,\ \chi)&=\left(\frac{N}{\pi}\right)^{s/2}\Gamma(s/2)\sum_{n=1}^{\infty}\chi(n)n^{-s}\\&=\int_0^{\infty}x^{s/2-1}\left(\sum_{n=1}^{\infty}\chi(n)e^{-n^2\pi x/N}\right)dx\\&=\frac{1}{2}\int_0^{\infty}x^{s/2-1}\psi(x,\ \chi)\,dx,\end{aligned}$$

其中 $\psi(x,\ \chi)=\sum\limits_{-\infty}^{\infty}\chi(n)e^{-n^2\pi x/N}$. 于是

$$\begin{aligned}G(1,\ \bar{\chi})\psi(x,\ \chi)&=\sum_{n=-\infty}^{\infty}G(1,\ \bar{\chi})\chi(n)e^{-n^2\pi x/N}\\&=\sum_{m=1}^{N}\bar{\chi}(m)\sum_{n=-\infty}^{\infty}e^{-\frac{n^2\pi x}{N}+2\pi i\frac{mn}{N}}.\end{aligned}\qquad (*)$$

在 Poisson 公式中取 $f(t)=e^{-\frac{t^2\pi x}{N}+2\pi i\frac{mt}{N}}$, 则其 Fourier 系数为

$$a_n=\int_{-\infty}^{\infty}e^{-\frac{t^2\pi x}{N}+2\pi i\frac{mt}{N}-2\pi int}\,dt=\sqrt{\frac{N}{x}}\,e^{-\frac{\pi}{Nx}(m-nN)^2}.$$

于是由 Poisson 公式可知(从(*)式)

$$\begin{aligned}G(1,\ \bar{\chi})\psi(x,\ \chi)&=\sum_{m=1}^{N}\bar{\chi}(m)\sqrt{\frac{N}{x}}\sum_{n=-\infty}^{\infty}e^{-\frac{\pi}{Nx}(nN+m)^2}\\&=\sqrt{\frac{N}{x}}\sum_{l=-\infty}^{\infty}\bar{\chi}(l)e^{-\frac{\pi l^2}{Nx}}\\&=\sqrt{\frac{N}{x}}\,\psi(x^{-1},\ \bar{\chi}).\end{aligned}$$

从而

$$\begin{aligned}\xi(s,\ \chi)&=\frac{1}{2}\int_1^{\infty}x^{s/2-1}\psi(x,\ \chi)\,dx+\frac{1}{2}\int_1^{\infty}x^{-s/2-1}\psi(x^{-1},\ \chi)\,dx\\&=\frac{1}{2}\int_1^{\infty}x^{s/2-1}\psi(x,\ \chi)\,dx\\&\quad+\frac{1}{2}\,\frac{\sqrt{N}}{G(1,\ \bar{\chi})}\int_1^{\infty}x^{\frac{1-s}{2}-1}\psi(x,\ \bar{\chi})\,dx.\end{aligned}$$

但是上式右边的积分对于任何 $s\in\mathbb{C}$ 均收敛．并且当 χ 为模 m 本原 D-特征时，$|G(1,\ \overline{\chi})|=\sqrt{N}\neq 0$．这就将 $\xi(s,\ \chi)$ 从而将 $L(s,\ \chi)$ 解析延拓到整个复平面，并且

$$\xi(1-s,\ \overline{\chi})=\frac{1}{2}\int_1^{\infty}x^{\frac{1-s}{2}-1}\psi(x,\ \overline{\chi})\mathrm{d}x$$

$$+\frac{1}{2}\frac{\sqrt{N}}{G(1,\ \chi)}\int_1^{\infty}x^{s/2-1}\psi(x,\ \chi)\mathrm{d}x$$

$$=\frac{\sqrt{N}}{G(1,\ \chi)}\xi(s,\ \chi),$$

其中用到公式 $G(1,\ \chi)G(1,\ \overline{\chi})=N\chi(-1)$．

(b) 若 χ 为奇特征，即 $\chi(-1)=-1$，此时 $\delta(\chi)=1$．而

$$\left(\frac{N}{\pi}\right)^{\frac{1}{2}(s+1)}\Gamma\left(\frac{1}{2}(s+1)\right)n^{-s}=\int_0^{\infty}ne^{-\frac{n^2\pi x}{N}}x^{\frac{1}{2}s-1/2}\,\mathrm{d}x,$$

从而

$$\left(\frac{N}{\pi}\right)^{\frac{1}{2}(s+1)}\Gamma\left(\frac{1}{2}(s+1)\right)L(s,\ \chi)=\frac{1}{2}\int_0^{\infty}\psi_1(x,\ \chi)x^{\frac{1}{2}(s-1)}\,\mathrm{d}x,$$

其中 $\psi_1(x,\ \chi)=\sum\limits_{n=-\infty}^{\infty}n\chi(n)e^{-n^2\pi x/N}$．由 Poisson 公式可得到

$$\sum_{n=-\infty}^{\infty}e^{-n^2\pi y+2\pi in\alpha}=y^{-1/2}\sum_{n=-\infty}^{\infty}e^{-(n+\alpha)^2\pi/y}\quad(y\neq 0),$$

对 α 微商给出

$$2\pi i\sum_{n=-\infty}^{\infty}ne^{-n^2\pi y+2\pi in\alpha}=-2\pi y^{-3/2}\sum_{n=-\infty}^{\infty}(n+\alpha)e^{-(n+\alpha)^2\pi/y}.$$

因此 $(y=x/N,\ \alpha=m/N)$

$$\sum_{n=-\infty}^{\infty}ne^{-\frac{n^2\pi x}{N}+\frac{2\pi imn}{N}}=i\left(\frac{N}{x}\right)^{3/2}\sum_{n=-\infty}^{\infty}\left(n+\frac{m}{N}\right)e^{-\pi\left(n+\frac{m}{N}\right)^2N/x}.$$

由此可得到 $G(1,\ \overline{\chi})\psi_1(x,\ \chi)=iN^{1/2}x^{-3/2}\psi_1(x^{-1},\ \overline{\chi})$．从而

$$\xi(s,\ \chi)=\frac{1}{2}\left[\int_1^{\infty}\psi_1(x,\ \chi)x^{-(1-s)/2}\mathrm{d}x\right.$$

$$\left.+\frac{1}{2}\frac{i\sqrt{N}}{G(1,\ \overline{\chi})}\int_1^{\infty}\psi_1(x,\ \overline{\chi})x^{-s/2}\mathrm{d}x\right]$$

于是又将 $L(s,\ \chi)$ 解析延拓到整个复平面上，并且由

$$G(1,\chi)\cdot G(1,\bar{\chi})=\chi(-1)N=-N$$

即可证得 $$\xi(1-s,\bar{\chi})=\frac{i\sqrt{N}}{G(1,\chi)}\xi(s,\chi).$$ ∎

引理 8 设 χ 为模 N 本原 D-特征. 则对任意 $t\in\mathbb{R}$, $L(1+it,\chi)\neq 0$.

证明 与证明引理 5 相仿, 当 $\sigma>1$, $s=\sigma+it$ 时,

$$\log L(s,\chi)=-\sum_p\log(1-\chi(p)p^{-s})=\sum_p\sum_{m=1}^{\infty}\chi(p)^m/mp^{ms}.$$

从而

$$\begin{aligned}&\zeta^3(\sigma)L^4(\sigma+it,\chi)L(\sigma+2it,\chi^2)\\&=\exp\left(\sum_p\sum_{m=1}^{\infty}\frac{3+4(\chi(p)p^{-it})^m+(\chi(p)p^{-it})^{2m}}{mp^{m\sigma}}\right),\end{aligned}$$

由于 $|\chi(p)p^{-it}|=1$, 从而可令 $\chi(p)p^{-it}=e^{i\theta}$. 于是

$$\begin{aligned}&\mathrm{Re}(3+4(\chi(p)p^{-it})^m+(\chi(p)p^{-it})^{2m})\\&=3+4\cos m\theta+\cos 2m\theta\\&=2(\cos m\theta+1)^2\geqslant 0.\end{aligned}$$

因此

$$\begin{aligned}&|\zeta^3(\sigma)L^4(\sigma+it,\chi)L(\sigma+2it,\chi^2)|\\&=\exp\left(\sum_p\sum_{m=1}^{\infty}\frac{2(\cos m\theta+1)^2}{mp^{m\sigma}}\right)\geqslant 1.\end{aligned}\qquad (*)$$

如果 $t\neq 0$ 或者 $t=0$ 而 $\chi^2\neq\chi_0$. 则 $1+2it$ 不是 $L(s,\chi^2)$ 的极点. 又知 1 为 $\zeta^3(s)$ 的 3 阶极点. 如果 $s=1+it$ 为 $L(s,\chi)$ 的零点, 则 $L^4(s,\chi)$ 在 $s=1+it$ 处至少有 4 阶零点. 从而当 $\sigma+it\to 1+it$ 时, (*)式左边→0 而右边≥1, 这就导致矛盾. 于是当 $t\neq 0$ 或者 $t=0$ 而 $\chi^2\neq\chi_0$ 时, $L(1+it,\chi)\neq 0$.

如果 $t=0$ 并且 $\chi^2=\chi_0$, 这时 χ 为实特值(即 χ 只取值 ±1). 我们考虑($\mathrm{Re}(s)>1$)

$$\begin{aligned}\zeta(s)L(s,\chi)&=\prod_p(1-p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1}\\&=\prod_{\chi(p)=0}(1-p^{-s})^{-1}\prod_{\chi(p)=1}(1-p^{-s})^{-2}\\&\quad\cdot\prod_{\chi(p)=-1}(1-p^{-2s})^{-1}\end{aligned}$$

$$
\begin{aligned}
&= \prod_{\chi(p)=0} (1+p^{-s}+p^{-2s}+\cdots) \\
&\quad \cdot \prod_{\chi(p)=1} (1+2p^{-s}+3p^{-2s}+\cdots) \\
&\quad \cdot \prod_{\chi(p)=-1} (1+p^{-2s}+p^{-4s}+\cdots) \\
&= \sum_{n=1}^{\infty} \rho(n) n^{-s}.
\end{aligned}
$$

可知 $\rho(n)\geqslant 0$，并且 $\rho(n^2)\geqslant 1$．如果 $L(1,\ \chi)=0$，则 $\zeta(s)L(s,\ \chi)$ 在 $\mathrm{Re}(s)>0$ 中正则．根据定理 2，$\sum\rho(n)n^{-s}$ 对于 $\sigma>0$ 收敛．但是在 $s=1/2$ 处：

$$\sum_{n=1}^{\infty} \rho(n)n^{-1/2}\geqslant \sum_{n=1}^{\infty} \rho(n^2)n^{-1}\geqslant \sum_{n=1}^{\infty} n^{-1}=\infty.$$

这就导致矛盾． ▌

引理 9 设 χ 是模 N 本原 D-特征，$N\geqslant 2$．则 $L(s,\ \chi)$ 是整个复平面上的解析函数．并且 $s=-\delta(\chi)-2n\ (n=0,\ 1,\ 2,\ \cdots)$ 是 $L(s,\ \chi)$ 的单零点，叫作是 $L(s,\ \chi)$ 的平凡零点．而 $L(s,\ \chi)$ 的其他零点均在带状区域 $0<\mathrm{Re}(s)<1$ 之内．

证明 由 $N\geqslant 2$ 而 χ 是模 N 本原特征，可知 $\chi\neq\chi_0$．由函数方程得到

$$
\begin{aligned}
L(s,\ \chi) &= \left(\frac{N}{\pi}\right)^{-s/2+(1-s)/2} \frac{\Gamma\left(\dfrac{1-s+\delta}{2}\right)}{\Gamma\left(\dfrac{s+\delta}{2}\right)} \\
&\quad \cdot L(1-s,\ \overline{\chi})\,\frac{G(1,\ \chi)}{i^{\delta}\sqrt{N}}. \qquad (*)
\end{aligned}
$$

注意 $|G(1,\ \chi)/i^{\delta}\sqrt{N}|=1$．当 $\mathrm{Re}(s)>0$ 时 $L(s,\ \chi)$ 没有奇点．当 $\mathrm{Re}(s)\leqslant 0$ 时，由 Gamma 函数的性质知上式右边无极点，从而 $L(s,\ \chi)$ 无极点，于是 $L(s,\ \chi)$ 是整个复平面上的解析函数．当 $\mathrm{Re}(s)>1$ 时 $L(s,\ \chi)$ 有收敛的 Euler 乘积展开式．从而 $L(s,\ \chi)\neq 0$，而当 $\mathrm{Re}(s)<0$ 时，考虑 $(*)$ 式右边可知 $L(s,\ \chi)$ 的零点只有 $\dfrac{s+\delta}{2}=0,\ -1,\ -2,\ \cdots$ 时，即 $s=-\delta-2n\ (n=0,\ 1,\ 2,\ \cdots)$．并且它们均是单零点．(包括 $s=0$ 的情形，因为已证了 $L(1,\ \overline{\chi})\neq 0$)

进而，引理 7 表明 $L(s, \chi)$ 在 $s=1+it(t\neq0)$ 处无零点，从而由函数方程可知在 $s=it(t\neq0)$ 处也无零点. 从而非平凡零点均在 $0<\mathrm{Re}(s)<1$ 之内. ∎

注记 所谓广义 **Riemann** 猜想即是：对于每个模 $N\geqslant2$ 本原 D-特征，$L(s, \chi)$ 的非平凡零点均在直线 $\mathrm{Re}(s)=\frac{1}{2}$ 之上!

2.4 Dirichlet 级数在负整数处的值，Bernoulli 数

定理 9 假设 $a_n\in\mathbb{C}(n=1, 2, \cdots)$，并且级数 $F(s)=\sum\limits_{n=1}^{\infty}a_nn^{-s}$ 的收敛横坐标 $\sigma_0<+\infty$. 令 $f(t)=\sum\limits_{n=1}^{\infty}a_ne^{-nt}$，则 $f(t)$ 在 $t>0$ 时收敛，并且

(a) 若 $t\to0$ 时 $f(t)$ 有如下的渐近展开：$f(t)\sim b_0+b_1t+b_2t^2+\cdots$（即意味着：对每个 N 均有 $f(t)=\sum\limits_{0\leqslant n<N}b_nt^n+O(t^N)$，$t\to0$），则 $F(s)$ 可以解析延拓成整个复平面上的全纯函数，并且 $F(-n)=(-1)^nn!\,b_n(n=0, 1, 2, \cdots)$.

(b) 如果 $f(t)$ 在 $t\to0$ 时有如下的渐近展开 $f(t)\sim\frac{b-1}{t}+b_0+b_1t+\cdots$，则 $F(s)$ 可以解析延拓到整个复平面上，$F(s)-\frac{b-1}{s-1}$ 为全纯函数，并且仍有 $F(-n)=(-1)^nn!\,b_n(n=0, 1, 2, \cdots)$.

证明 由于 $\sigma_0<+\infty$，可知 $A(N)=\sum\limits_{n=1}^{N}a_n=O(N^{\sigma_0+\varepsilon})$（定理 1）. 从而 $a_n=A(n)-A(n-1)=O(n^{\sigma_0+\varepsilon})$，由此即知

$$f(t)=\sum_{n=1}^{\infty}a_ne^{-nt}.$$

在 $t>0$ 时收敛. 考虑（$\mathrm{Re}(s)>\sigma_0+1$）：

$$\begin{aligned}\Gamma(s)F(s)&=\int_0^{\infty}t^{s-1}e^{-t}\sum_{n=1}^{\infty}a_nn^{-s}\,\mathrm{d}t=\int_0^{\infty}t^{s-1}\sum_{n=1}^{\infty}a_ne^{-nt}\,\mathrm{d}t\\&=\int_0^{\infty}t^{s-1}f(t)\,\mathrm{d}t=\int_1^{\infty}+\int_0^{1}.\end{aligned}$$

由 $f(t)$ 的解析特性知积分 $\int_1^{\infty}$ 在整个 s 平面上全纯. 另一方面，

由 $f(t)=\sum\limits_{n<N} b_n t^n + O(t^N)$，可知

$$\int_0^1 f(t)t^{s-1}\,\mathrm{d}t=\sum_{n<N}\frac{b_n}{s+n}+\int_0^1\Big(f(t)-\sum_{n<N}b_n t^n\Big)t^{s-1}\,\mathrm{d}t.$$

当 $\mathrm{Re}(s)>-N$ 时，后边积分收敛，从而

$$\Gamma(s)F(s)=\sum_{n<N}\frac{b_n}{s+n}+G(s), \qquad (*)$$

$G(s)$ 在 $\mathrm{Re}(s)>-N$ 中正则。由于 N 可取充分大的整数，从而 $F(s)$ 由此解析延拓到整个复平面上。

(a) 若 $f(t)\sim b_0+b_1t+b_2t^2+\cdots$，$(t\to 0)$ 则 $(*)$ 式右边在 $s=0, -1, -2, \cdots$ 有一阶极点，而 $\Gamma(s)$ 也恰好如此。因此 $F(s)$ 在整个复平面上全纯，并且

$$F(-n)=b_n/\operatorname*{res}_{s=-n}\Gamma(s)=(-1)^n n!\,b_n. \quad (n=0, 1, 2, \cdots).$$

(b) 若 $f(t)\sim\dfrac{b-1}{t}+b_0+b_1t+\cdots(t\to 0)$，则 $(*)$ 式右边第一项为 $(b-1)/(s-1)$，而 $\Gamma(1)=1$，从而 $F(s)-(b-1)/(s-1)$ 在整个复平面上全纯，并且仍有

$$F(-n)=b_n/\operatorname*{res}_{s=-n}\Gamma(s)=(-1)^n n!\,b_n \quad (n=0, 1, 2, \cdots). \blacksquare$$

现在我们用此定理求 $\zeta(s)$ 和 $L(s, \chi)$ 在 $s=n$ $(n=0, -1, -2, \cdots)$ 处的值。这些值用 Bernoulli 数和广义 Bernoulli 数来表达。我们先介绍这些数。

定义 6 由下面 Taylor 展开式定义的系数 B_n 叫作是 **Bernoulli 数**。

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n.$$

B_n 的前几个值为

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$

对于 $n\geqslant 0$，$B_n(x)=\sum\limits_{k=0}^{n}\binom{n}{k}B_{n-k}x^k$ 叫作是 **Bernoulli 多项**

式. 例如: $B_0(x)=1$, $B_1(x)=x-\frac{1}{2}$, $B_2(x)=x^2-x+\frac{1}{6}$, $B_3(x)=x^3-\frac{3}{2}x^2+\frac{1}{2}x$, ….

最后, 设 χ 是模 N 的 D-特征, 定义广义 Bernoulli 数为

$$B_{n,\chi}=N^{n-1}\sum_{m=1}^{N}\chi(m)B_n\left(\frac{m}{N}\right).$$

其中 $B_n\left(\frac{m}{N}\right)$为 Bernoulli 多项式 $B_n(x)$在 $x=\frac{m}{N}$ 处的值

定理 10 (Bernoulli 数的基本性质).

(a) 符号地定义$(1+B)^n=\sum_{k=0}^{n}\binom{n}{k}B_k$, 则当 $n\geqslant 2$ 时$(1+B)^n=B_n$. 从而得到递归公式:

$$-nB_{n-1}=B_0+\binom{n}{1}B_1+\cdots+\binom{n}{n-2}B_{n-2}\quad (n\geqslant 2).$$

由此可知 $B_n\in\mathbb{Q}$.

(b) $\frac{te^{xt}}{e^t-1}=\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}t^n$, $\frac{t}{e^{Nt}-1}\sum_{m=1}^{N}\chi(m)e^{mt}=\sum_{n=0}^{\infty}\frac{B_{n,\chi}}{n!}t^n$ ($\chi\neq\chi_0$时).

(c) $B_1=-1/2$, 而当 $2\nmid n\geqslant 3$ 时, $B_n=0$.

若 $\chi\neq\chi_0$, $n\geqslant 1$, 则 $\delta(\chi)+n\equiv 1 \pmod 2$时 $B_{n,\chi}=0$.

证明

(a) 由 B_n 的定义即知

$$\begin{aligned}t&=\left(\sum_{n=0}^{\infty}t^n/n!\right)\left(\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n\right)-\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n\\&=\sum_{n=0}^{\infty}t^n\sum_{k+l=n}\frac{B_k}{k!\,l!}-\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n\\&=\sum_{n=0}^{\infty}\frac{t^n(1+B)^n}{n!}-\sum_{n=0}^{\infty}\frac{B_n}{n!}t^n.\end{aligned}$$

比较 t^n 的系数, 便知当 $n\geqslant 2$ 时, $B_n=(1+B)^n$. 由此不难得到(a)中的其他结论.

(b) $\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}t^n=\sum_{n=0}^{\infty}\frac{t^n}{n!}\sum_{k=0}^{n}\binom{n}{k}B_kx^{n-k}$

$$= \sum_{n=0}^{\infty} \sum_{k+l=n} \frac{B_k t^k}{k!} \frac{x^l t^l}{l!}$$

$$= \left(\sum_{k=1}^{\infty} \frac{B_k}{k!} t^k\right)\left(\sum_{l=1}^{\infty} \frac{1}{l!} (xt)^l\right) = \frac{te^{xt}}{e^t - 1}.$$

$$\sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n = \sum_{n=0}^{\infty} \frac{t^n}{n!} N^{n-1} \sum_{m=1}^{N} \chi(m) B_n\left(\frac{m}{N}\right)$$

$$= \frac{1}{N} \sum_{m=1}^{N} \chi(m) \sum_{n=0}^{\infty} \frac{B_n\left(\frac{m}{N}\right)}{n!} (tN)^n$$

$$= \frac{1}{N} \sum_{m=1}^{N} \chi(m) \frac{Nte^{mt}}{e^{Nt} - 1}$$

$$= \frac{t}{e^{Nt} - 1} \sum_{m=1}^{N} \chi(m) e^{mt}.$$

(c) $$2 \sum_{\substack{n=0 \\ 2\nmid n}}^{\infty} \frac{B_n}{n!} t^n = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n - \sum_{n=0}^{\infty} \frac{B_n}{n!} (-t)^n$$

$$= \frac{t}{e^t - 1} - \frac{-t}{e^{-t} - 1} = -t.$$

于是 $B_1 = -1/2$，而当 $2\nmid n \geqslant 3$ 时，$B_n = 0$. 对于广义 Bernoulli 数，当 $\chi(-1) = 1$ 时

$$2 \sum_{\substack{n=0 \\ 2\nmid n}}^{\infty} \frac{B_{n,\chi}}{n!} t^n = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n - \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} (-t)^n$$

$$= \frac{t}{e^{Nt} - 1}\left(\sum_{m=1}^{N} \chi(m) e^{mt} - \sum_{m=1}^{N} \chi(m) e^{-mt}\right)$$

$$= \frac{t}{e^{Nt} - 1}\left(\sum_{m=1}^{N} \chi(m) e^{mt} - \sum_{m=1}^{N} \chi(-m) e^{mt}\right) = 0.$$

因此在 $\chi(-1) = 1$ 而 $2\nmid n$ 时，$B_{n,\chi} = 0$. 同样可证在 $\chi(-1) = -1$ 而 $2|n$ 时 $B_{n,\chi} = 0$. ∎

现在我们求 $\zeta(s)$ 和 $L(s,\chi)$ 在负整数处的值. 我们同时又(不用函数方程)给出它们在整个复平面上的解析延拓.

定理 11 (a) 令 $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ ($\mathrm{Re}(s) > 1$). 则 $\zeta(s) - \frac{1}{s-1}$ 可解析延拓成整个复平面上的全纯函数，并且 $\zeta(0) = -1/2$，而当 $n \geqslant 1$ 时，$\zeta(-n) = -\frac{B_{n+1}}{n+1}$.

(b) 设 χ 为模 N 的 D-特征，则

$$L(s,\ \chi)=\sum_{n=0}^{\infty}\chi(n)n^{-s}\quad(\mathrm{Re}(s)>1)$$

可解析延拓成整个复平面上的亚纯函数. 进而，若 $\chi\neq\chi_0$，则 $L(s,\ \chi)$在整个复平面上全纯. 而 $\chi=\chi_0$ 时只有 $s=1$ 是 $L(s,\ \chi_0)$ 的极点并且是单极点，$\underset{s=1}{\mathrm{res}}\,L(s,\ \chi_0)=\varphi(N)/N$. 最后，

$$L(-n,\ \chi)=-\frac{B_{n+1,\chi}}{n+1}\quad(n=0,\ 1,\ 2,\ \cdots).$$

证明

(a) 在定理 8 中取 $F(s)=\zeta(s)$，则 $a_n\equiv1$. 于是

$$f(t)=\sum_{n=1}^{\infty}a_ne^{-nt}=\frac{1}{e^t-1}\sim\frac{1}{t}+\sum_{n=0}^{\infty}\frac{B_{n+1}}{(n+1)!}t^n\quad(t\to0),$$

从而由定理 8 即得(a)中的结论.

(b) 在定理 8 中取 $a_n=\chi(n)$. 这时

$$\begin{aligned}f(t)&=\sum_{n=1}^{\infty}\chi(n)e^{-nt}=\sum_{m=1}^{N}\chi(m)\sum_{n=0}^{\infty}e^{-(m+nN)t}\\&=\sum_{m=1}^{N}\chi(m)\frac{e^{-mt}}{1-e^{-Nt}}\\&=\sum_{m=1}^{N-1}\chi(m)\left(\sum_{k=0}^{\infty}(-1)^k\frac{m^k}{k!}t^k\right)\left(\sum_{r=0}^{\infty}\frac{(-1)^rB_r}{r!}(Nt)^{r-1}\right)\\&=\sum_{m=1}^{N-1}\chi(m)\sum_{k,r=0}^{\infty}\frac{(-1)^{k+r}m^kN^{r-1}B_r}{k!r!}t^{k+r-1}.\end{aligned}$$

当 $t\to0$ 时，$f(t)$的渐近展开式中 t^n 项系数为

$$b_n=\sum_{m=1}^{N-1}\chi(m)\sum_{\substack{k,r\geq0\\k+r=n+1}}\frac{(-1)^{n+1}m^kN^{r-1}B_r}{k!r!}$$

$$(n=-1,\ 0,\ 1,\ \cdots).$$

当 $n=-1$ 时，

$$b_{-1}=\frac{1}{N}\sum_{m=1}^{N-1}\chi(m)=\begin{cases}0, & \chi\neq\chi_0\text{时};\\ \varphi(N)/N, & \chi=\chi_0\text{时}.\end{cases}$$

而当 $n\geq0$ 时，

$$b_n=\frac{(-1)^{n+1}}{(n+1)!}N^n\sum_{m=1}^{N}\chi(m)\sum_{k=0}^{n+1}\binom{n+1}{k}\left(\frac{m}{N}\right)^k B_{n+1-k}$$
$$=\frac{(-1)^{n+1}}{(n+1)!}N^n\sum_{m=1}^{N}\chi(m)B_{n+1}\left(\frac{m}{N}\right)$$
$$=\frac{(-1)^{n+1}}{(n+1)!}B_{n+1,\chi}.$$

于是由定理 8 即知

$$L(-n,\chi)=(-1)^n n!\,b_n=-\frac{B_{n+1,\chi}}{n+1},\ (n=0,1,2,\cdots)$$

并且(b)中其他结论也是对的. ∎

习　　题

1. 利用函数方程计算 $\zeta(0)$ 和 $\zeta(-1)$.
2. 求证: (a) $\xi(s)=\frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$ 是复平面上的全纯函数, 并且 $\xi(s)=\xi(1-s)$.
   (b) $\xi(s)$ 的全部零点均在带状区域 $0<\mathrm{Re}(s)<1$ 之内, 并且零点对于直线 $\mathrm{Im}(s)=0$(实轴)和 $\mathrm{Re}(s)=\frac{1}{2}$ 均是对称的.
3. 求证当 $n=1,3,5,7,\cdots$ 时 $\zeta(1-2n)<0$, 而当 $n=2,4,6,8,\cdots$ 时, $\zeta(1-2n)>0$.
4. 设 H 是有限 Abel 群 G 的子群. 求证 $H^{\perp}=\{\chi\in\hat{G}\,|\,\chi(H)=1\}$ 是 $\hat{G}$ 的子群, 并且 $H^{\perp}$ 同构于 G/H.
5. (正交关系的矩阵形式). 设 $G=\{g_1,\cdots,g_n\}$ 为有限 Abel 群, $\hat{G}=\{\chi_1,\cdots,\chi_n\}$. $A=(a_{ij})$ 为 n 阶复方阵, $a_{ij}=\chi_i(g_j)$. 求证 $A^*A=AA^*=nI_n$. 其中 $A^*=(\bar{a}_{ji})$ 而 I_n 为 n 阶单位方阵.
6. 设 $G=\{g_1,\cdots,g_n\}$ 为 n 阶 Abel 群, $\{a_{g_1},\cdots,a_{g_n}\}$ 为 n 个复数. 定义 n 阶复方阵 $A=(a_{ij})$, 其中 $a_{ij}=a_{g_ig_j}(1\leqslant i,j\leqslant n)$. 求证
$$\det A=\prod_{\chi\in\hat{G}}\Big(\sum_{g\in G}a_g\chi(g)\Big).$$
7. (a) 对于 $n=4$ 和 6, 用上题计算
$$A_n=\begin{pmatrix}a_0 & a_1 & a_2 & \cdots & a_{n-1}\\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_1 & a_2 & a_3 & \cdots & a_0\end{pmatrix}$$

的行列式；

(b) 计算$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$的行列式。

8. 对于 $m=3, 7, 12$，写出模 m 的全部加法特征和 D-特征。

9. 设 p 为奇素数，求证 Legendre 符号 $\left(\frac{\ }{p}\right)$: $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ 是模 p 的 D-特征，并且是模 m 唯一的非平凡实特征。如果 χ 为 $(\mathbb{Z}/p\mathbb{Z})^*$ 的特征群的生成元，试问 $\left(\frac{\ }{p}\right)$ 为 χ 的多少次方？

10. 当 $m\geqslant 3$ 时，求证在模 m 的 D-特征中，奇特征与偶特征各占一半。

11. 设 χ 为模 m 的 D-特征并且 $\chi\neq\chi_0$。对于 $(m, a)>1$，规定 $\chi(a)=0$。求证：对于任意 $a, b\in\mathbb{Z}$ 均有 $\left|\sum\limits_{n=a}^{b}\chi(n)\right|\leqslant\varphi(m)/2$。

12. $m\geqslant 3$，求证（左边求和过模 m 的全部奇 Dirichlet 特征）

$$\sum_{\substack{\chi \\ \chi(-1)=-1}}\chi(n)=\begin{cases} \frac{1}{2}\varphi(m), & \text{当 } n\equiv 1(\operatorname{mod} m)\text{ 时；} \\ -\frac{1}{2}\varphi(m), & \text{当 } n\equiv -1(\operatorname{mod} m)\text{ 时；} \\ 0, & \text{否则。} \end{cases}$$

13. (a) 若 χ 为模 m 的偶 Dirichlet 特征，$\chi\neq\chi_0$，则 $\sum\limits_{a=0}^{m-1}\chi(a)a=0$；

(b) 若 χ 为模 m 的奇 Dirichlet 特征，则 $\sum\limits_{a=1}^{m-1}\chi(a)a^2=m\sum\limits_{a=1}^{m-1}\chi(a)a$。

14. (a) 列出模 10 的全部 D-特征，求出它们的导子。试问哪些是本原的？

(b) 列出 $\operatorname{cond}(\chi)=3$ 的全部模 9 的 D-特征 χ。

15. 以 $f(m)$ 表示模 m 的本原 D-特征个数，求证：

(a) $f(m)$ 是积性数论函数（参考第 19 题）；

(b) $f(p^n)=\varphi(p^n)-\varphi(p^{n-1})$；

(c) $f(m)=0\Leftrightarrow m\equiv 2(\operatorname{mod} 4)$。

16. （有限 Fourier 变换）假设 $a_1, \cdots, a_m, c_1, \cdots, c_m\in\mathbb{C}$，则

$$c_\lambda=\sum_{n=1}^{m}a_n e^{2\pi in\lambda/m}(1\leqslant\lambda\leqslant m)\Leftrightarrow a_\mu=\frac{1}{m}\sum_{n=1}^{m}c_\lambda e^{-\frac{2\pi i n\mu}{m}}(1\leqslant\mu\leqslant m)。$$

17. 设 $f(x)\in\mathbb{Z}[x]$，

(a) 以 $N_m(n)$ 表示同余方程 $f(x)\equiv n(\operatorname{mod} m)$ 的模 m 解的个数。求证：

$$N_m(n)=\frac{1}{m}\sum_{\lambda=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i(f(x)-n)\lambda/m}；$$

(b) 以 $N_M(n)$ 表示方程 $f(x)=n$，$|x|\leqslant M$ 的有理整数解的个数。求证

$$N_M(n)=\int_0^1\sum_{x=-M}^{M}e^{2\pi i(f(x)-n)y}\mathrm{d}y.$$

以上两个公式是解析数论中指数和方法的起点.

18. (a) 设 p 为奇素数. $f(x)=(ax+b)x$, $a, b\in\mathbb{Z}$. $(a, p)=(b, p)=1$. 求证: $\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)=-\left(\frac{a}{p}\right)$;

(b) 设 p 为奇素数, $\alpha, \beta\in\{\pm1\}$. 定义

$$S(\alpha, \beta)=\left\{x\,\middle|\,1\leqslant x\leqslant p-2, \left(\frac{x}{p}\right)=\alpha, \left(\frac{x+1}{p}\right)=\beta\right\},$$

$$N(\alpha, \beta)=|S(\alpha, \beta)|.$$

求证: $N(\alpha, \beta)=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\alpha\left(\frac{x}{p}\right)\right)\left(1+\beta\left(\frac{x+1}{p}\right)\right)$;

(c) 求证:

$$N(1, 1)=\frac{1}{4}\left(p-4-\left(\frac{-1}{p}\right)\right),$$

$$N(1, -1)=1+N(1, 1),$$

$$N(-1, -1)=N(-1, 1)=\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right).$$

19. 设 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ 是 $m\geqslant2$ 的素因子分解式. 求证: 每个模 m 的 D-特征均可唯一地写成 $\chi=\chi_1\cdots\chi_r$, 其中 χ_i 为模 $p_i^{\alpha_i}$ 的 D-特征($1\leqslant i\leqslant r$), 进而: χ 为模 m 的本原 D-特征 $\Leftrightarrow$ 每个 χ_i 均是模 $p_i^{\alpha_i}$ 的本原 D-特征($1\leqslant i\leqslant k$).

20. 设 χ 为模 4 (唯一的)本原 D-特征. 试计算 $L(1, \chi)$和 $L(0, \chi)$.

21. 求证当 $n\geqslant1$ 时, $B_{4n}<0$, $B_{4n-2}>0$.

22. 求证 $1^n+2^n+\cdots+N^n=\frac{1}{n+1}(B_{n+1}(N+1)-B_{n+1})$, 其中 $B_{n+1}(N+1)$ 是 Bernoulli 多项式 $B_{n+1}(x)$在 $x=N+1$ 处的取值.

23. 当 $k\geqslant1$ 时, 求证 $\zeta(2k)=(-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2\cdot(2k)!}$.

24. 设 χ 为模 m 的 D-特征, $\chi\neq\chi_0$. 求证 $L(0, \chi)=-\frac{1}{m}\sum_{n=1}^{m}\chi(n)n$.

25. 设 χ 为模 m 的本原 D-特征. 求证 $G(1, \chi)G(1, \bar{\chi})=\chi(-1)m$.

26. 设 G 为 fg 阶 Abel 群, a 为 G 中一个 f 阶元素, 则

$$\prod_{\chi\in\hat{G}}(1-\chi(a)x)=(1-x^f)^g.$$

§ 3 Dedekind zeta 函数 $\zeta_K(s)$

3.1 留数公式

现在我们将 Dirichlet 和 Riemann 开创的解析方法用于代数数论. 对于代数数论中的许多本质性问题(如本书第五章中关于素理想分解和密度问题,第六章中的类数问题,以及本书中未讲到的类域论的建立等),解析方法都作出了重要的贡献.

仿照域 $\mathbb{Q}$ 上的 Riemann zeta 函数 $\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$, Dedekind 对于每个代数数域 K,定义了 Dirichlet 级数

$$\zeta_k(s)=\sum_{\mathfrak{a}}N(\mathfrak{a})^{-s},$$

其中 $\mathfrak{a}$ 过数域 K 的全部非零整理想, $N(\mathfrak{a})=N_{K/\mathbb{Q}}(\mathfrak{a})$, 称 $\zeta_K(s)$ 为数域 K 的 Dedekind zeta 函数. 如果以 a_n 表示 O_K 中范为 n 的整理想个数, 则 $\zeta_K(s)=\sum_{n=1}^{\infty}a_n n^{-s}$, 从而 $\zeta_K(s)$ 不过是数论函数 a_n 的 Dirichlet 级数. 按照前面的研究程序, 下一步自然需要考查 $\zeta_K(s)$ 的解析特性. 我们先来证明它的收敛横坐标 $\sigma_0\leqslant 1$.

定理 12

(a) 级数 $\zeta_K(s)=\sum_{\mathfrak{a}}N(\mathfrak{a})^{-s}$ 有如下性质:

(P) 在 $\mathrm{Re}(s)>1$ 中收敛, 并且在半平面 $\mathrm{Re}(s)>1$ 的每个紧子集中一致绝对收敛(从而在 $\mathrm{Re}(s)>1$ 中定义出正则函数).

(b) 当 $\mathrm{Re}(s)>1$ 时, 无穷乘积 $\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$ 收敛, 并且有 Euler 乘积展开式 $\zeta_K(s)=\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$, 其中 $\mathfrak{p}$ 过 O_K 的全部素理想.

证明

(a) 令 $n=[K:\mathbb{Q}]$. 由于每个有理素数 p 在 K 中至多有 n 个素理想因子 $\left(g\leqslant\sum_{i=1}^{g}e_i f_i\leqslant n\right)$, 从而当 $\sigma>1$ 时,

$$\sum_{N(\mathfrak{p})\leqslant x} N(\mathfrak{p})^{-\sigma}\leqslant\sum_{p\leqslant x}\sum_{\mathfrak{p}|p} N(\mathfrak{p})^{-\sigma}\leqslant n\sum_{p\leqslant x} p^{-\sigma}\leqslant n\sum_{m\leqslant x} m^{-\sigma}.$$

这就表明 D-级数 $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$ 有性质 (P). 进而，当 $\sigma>1$ 时

$$\sum_{N(\mathfrak{p})\leqslant x}\sum_{m=1}^{\infty} N(\mathfrak{p})^{-m\sigma}=\sum_{N(\mathfrak{p})\leqslant x} N(\mathfrak{p})^{-\sigma}(1-N(\mathfrak{p})^{-\sigma})^{-1}$$
$$\leqslant 2\sum_{N(\mathfrak{p})\leqslant x} N(\mathfrak{p})^{-\sigma},$$

从而 $\sum_{\mathfrak{p}}\sum_{m=1}^{\infty} N(\mathfrak{p})^{-ms}$ 也有性质 (P). 于是无穷乘积 $\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$ 也有性质 (P). 进而，由 O_K 中素理想唯一分解性质，可知当 $\sigma>1$ 时，

$$\prod_{N(\mathfrak{p})\leqslant x}(1-N(\mathfrak{p})^{-\sigma})^{-1}=\prod_{N(\mathfrak{p})\leqslant x}(1+N(\mathfrak{p})^{-\sigma}+N(\mathfrak{p})^{-2\sigma}+\cdots)$$
$$\geqslant\sum_{N(\mathfrak{a})\leqslant x} N(\mathfrak{a})^{-\sigma}.$$

这就证明了 $\zeta_K(s)=\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ 也有性质 (P).

(b) 我们已经证明了 $\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$ 有性质 (P). 另一方面，

$$\prod_{N(\mathfrak{p})\leqslant x}(1-N(\mathfrak{p})^{-s})^{-1}=\sum_{N(\mathfrak{a})\leqslant x} N(\mathfrak{a})^{-s}+\sum_{N(\mathfrak{a})>x}{}' N(\mathfrak{a})^{-s},$$

从而当 $\mathrm{Re}(s)=\sigma>1$ 时，

$$\Big|\prod_{N(\mathfrak{p})\leqslant x}(1-N(\mathfrak{p})^{-s})^{-1}-\sum_{N(\mathfrak{a})\leqslant x} N(\mathfrak{a})^{-s}\Big|$$
$$\leqslant\sum_{N(\mathfrak{a})>x} N(\mathfrak{a})^{-\sigma}\to 0\quad(\text{当 } x\to\infty).$$

这就证明了在 $\mathrm{Re}(s)>1$ 时，$\zeta_K(s)=\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$. ∎

注记 设 C 是数域 K 的任意一个理想类，定义

$$\zeta_K(C,s)=\sum_{\mathfrak{a}\in C} N(\mathfrak{a})^{-s}=\sum_{n=1}^{\infty} a_n(C)n^{-s}.$$

其中 $\mathfrak{a}$ 过理想类 C 中全部非零整理想，而 $a_n(C)$ 表示类 C 中范为 n 的整理想个数. 显然 $\zeta_K(s)=\sum_{C\in C(K)}\zeta_K(C,s)$，并且由于正项级数 $\sum_{n=1}^{\infty} a_n(C)n^{-s}$ 的系数小于 $\sum_{n=1}^{\infty} a_n n^{-s}=\zeta_K(s)$ 中相应的系数，从而由定理 1 知 $\zeta_K(C,s)$ 也有性质 (P).

现在考虑 $\zeta_K(C,s)$ 和 $\zeta_K(s)$ 在 $s=1$ 处的性状. 我们要证 $s=1$

为 $\zeta_K(C, s)$ 和 $\zeta_K(s)$ 的一阶极点，因此 $\sigma_0=1$. 根据 D-级数的一般理论，σ_0 和 $\zeta_K(C, s)$ 在 $\sigma_0=1$ 的留数与部分和 $\sum\limits_{n=1}^{N} a_n(C)$ 的大小有关. 正是在这一点上，解析理论与代数数论发生了深刻的联系. 因为下面定理显示出，在 $\sum\limits_{n=1}^{N} a_n(C)$ 公式的主项中几乎包含了我们在本书第 I 部分得到的数域 K 的全部不变量，而定理的证明本身也显示出我们需要借助代数数论中多么广泛的知识.

定理 13 设 C 是代数数域 K 的一个理想类，$n=[K:\mathbb{Q}]$. 令

$$f(C, x)=\sum_{\substack{\mathfrak{a}\in C\\ N(\mathfrak{a})\leqslant x}} 1=\sum_{n\leqslant x} a_n(C)$$

其中 $\mathfrak{a}$ 过范 $\leqslant x$ 并且属于类 C 的整理想. 则当 $x\to\infty$ 时，

$$f(C, x)=\rho_K x+O(x^{1-\frac{1}{n}}),\quad \rho_K=\frac{2^{r_1}(2\pi)^{r_2}R_K}{w_K\cdot\sqrt{|d(K)|}},$$

其中 r_1 和 r_2 分别是 K 到 $\mathbb{C}$ 中的实嵌入个数和复嵌入对数，R_K 和 $d(K)$ 分别是 K 的 regulator 和判别式，w_K 是 K 中单位根群 W_K 的阶.

证明 第一步(理想求和化为元素求和). 先在理想类 C^{-1} 中任取一个整理想 $\mathfrak{B}$. 如果 $\mathfrak{a}$ 为 C 中的整理想，则 $\mathfrak{a}\mathfrak{B}=(\alpha), \alpha\in\mathfrak{B}$. $N(\alpha)=N(\mathfrak{a})N(\mathfrak{B})\leqslant xN(\mathfrak{B})$. 反之，如果 $\alpha\in\mathfrak{B}$, $N(\alpha)\leqslant xN(\mathfrak{B})$，则 $\mathfrak{a}=(\alpha)\mathfrak{B}^{-1}$ 为整理想，并且 $N(\mathfrak{a})=N(\alpha)N(\mathfrak{B})^{-1}\leqslant x$. 从而 $f(C, x)$ 等于主理想集合 $\{(\alpha)=\alpha O_K \mid \alpha\in\mathfrak{B},\ N(\alpha)\leqslant x\cdot N(\mathfrak{B})\}$ 中主理想个数. 由于 $(\alpha)=(\beta)\Leftrightarrow\alpha/\beta\in U_K$，于是

$$f(C, x)=\#\{\alpha(\mathrm{mod}\,U_K)\mid\alpha\in\mathfrak{B},\ N(\alpha)\leqslant xN(\mathfrak{B})\},\tag{1}$$

其中 $\alpha(\mathrm{mod}\,U_K)$ 表示在每个集合 αU_K 中取一个元素，而 $\#A=|A|$. 设 $\alpha_1, \cdots, \alpha_n$ 是 Abel 群 $\mathfrak{B}$ 的一组基，则 $\mathfrak{B}$ 中每个元素唯一地表示成 $\alpha=\sum\limits_{i=1}^{n} m_i\alpha_i\ (m_i\in\mathbb{Z})$. 作映射

$$\varphi:\ \mathfrak{B}\to\mathbb{R}^n,\ \alpha=\sum_{i=1}^{n} m_i\alpha_i\mapsto(m_1, \cdots, m_n),\tag{2}$$

则 $\varphi(\mathfrak{B})$ 为 $\mathbb{R}^n$ 中的格，于是公式(1)可写成

$$f(C,\ x)=\#\left\{(x_1,\ \cdots,\ x_n)\in\mathbb{Z}^n\,\middle|\,\alpha=\sum_{i=1}^{n}x_i\alpha_i(\operatorname{mod}U_K),\right.$$

$$\left.0<N(\alpha)\leqslant xN(\mathfrak{B})\right\}\tag{3}$$

第二步(处理单位群)接下来要应用 Dirichlet 单位定理. 这个定理是说: $U_K=W_K\times V_K$, 其中 W_K 是 K 的单位根群, V_K 是秩 $r=r_1+r_2-1$ 的自由 Abel 群, 并且 V_K 以一组基本单位 $\varepsilon_1,\ \cdots,\ \varepsilon_r$ 为基. 考虑映射

$$K^*\xrightarrow{\sigma}\mathbb{R}^{*r_1}\times\mathbb{C}^{*r_2}\xrightarrow{l}\mathbb{R}^{r_1+r_2}$$

其中 $\sigma(\alpha)=(\sigma_1(\alpha),\ \cdots,\ \sigma_{r_1+r_2}(\alpha))$ $(\sigma_1,\ \cdots,\ \sigma_{r_1+r_2}$ 是 K 到 $\mathbb{C}$ 中的前 r_1+r_2 个嵌入), 而

$$l(y_1,\ \cdots,y_{r_1+r_2})=(n_1\log|y_1|,\ \cdots,\ n_{r_1+r_2}\log|y_{r_1+r_2}|)$$

为对数映射, $n_i=1(1\leqslant i\leqslant r_1)$、$2(r_1+1\leqslant i\leqslant r_1+r_2)$. 我们已经知道:

(i) $\ker(l\circ\sigma)=W_K$;

(ii) $l\circ\sigma(V_K)$ 为 $\mathbb{R}^{r_1+r_2}$ 的超平面

$$H=\{(x_1,\ \cdots,\ x_{r_1+r_2})\in\mathbb{R}^{r_1+r_2}\,|\,x_1+\cdots+x_{r_1+r_2}=0\}$$

中的格, 并且此格以 $l\circ\sigma(\varepsilon_1),\ \cdots,\ l\circ\sigma(\varepsilon_r)$ 为基. 令

$$t=(n_1,\ \cdots,\ n_{r_1+r_2})\in\mathbb{R}^{r_1+r_2},$$

显然 $t\notin H$. 从而 $t,\ l\circ\sigma(\varepsilon_1),\ \cdots,\ l\circ\sigma(\varepsilon_r)$ 形成实向量空间 $\mathbb{R}^{r_1+r_2}$ 的一组基. 即

$$\mathbb{R}^{r_1+r_2}=\mathbb{R}t\oplus\mathbb{R}l\circ\sigma(\varepsilon_1)\oplus\cdots\oplus\mathbb{R}l\circ\sigma(\varepsilon_r).$$

对于每个 $\alpha\in K^\times=K-\{0\}$, $l\circ\sigma(\alpha)\in\mathbb{R}^{r_1+r_2}$, 从而唯一地写成

$$l\circ\sigma(\alpha)=ct+\sum_{i=1}^{r}c_il\circ\sigma(\varepsilon_i)\qquad c,\ c_i\in\mathbb{R}.$$

而每个单位唯一地写成 $u=w\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$, $w\in W_K$, $a_i\in\mathbb{Z}$. 于是

$$l\circ\sigma(u\alpha)=ct+\sum_{i=1}^{r}(c_i+a_i)l\circ\sigma(\varepsilon_i).$$

这就表明, 对于每个 $\alpha=\sum\limits_{i=1}^{n}x_i\alpha_i\in\mathfrak{B}-\{0\}$, $x_i\in\mathbb{Z}$, 在 αU_K 中可选取恰好 w_K 个元素 $\alpha uw(w\in W_K)$, 使得 $0\leqslant c_i+a_i<1(1\leqslant i\leqslant r)$. 从

而(3)式又可化为

$$w_K f(C, x)=\#\Big\{(x_1, \cdots, x_n)\in\mathbb{Z}^n \Big| \alpha=\sum_{i=1}^n x_i\alpha_i,\ 0<N(\alpha)$$

$$\leqslant xN(\mathfrak{B}), l\circ\sigma(\alpha)=ct+\sum_{i=1}^r c_i l\circ\sigma(\varepsilon_i),$$

$$c,\ c_i\in\mathbb{R},\ 0\leqslant c_i\leqslant 1\ (1\leqslant i\leqslant r)\Big\} \qquad (4)$$

对于 $y=(y_1, \cdots, y_{r_1+r_2})\in\mathbb{R}^{r_1}\times C^{r_2}$,我们定义

$$N(y)=|y_1\cdots y_{r_1}y_{r_1+1}^2\cdots y_{r_1+r_2}^2|,$$

则
$$N(\sigma(\alpha))=N\Big(\sum_{i=1}^n x_i\sigma(\alpha_i)\Big).$$

注意当 $\alpha\in K$ 时, $N(\sigma(\alpha))$ 与普通的范 $N(\alpha)$ 一致. 又定义

$$\Gamma_0=\Big\{(x_1, \cdots, x_n)\in\mathbb{R}^n \Big| 0<N\Big(\sum_{i=1}^n x_i\sigma(\alpha_i)\Big)\leqslant 1,$$

$$l\Big(\sum_{i=1}^n x_i\sigma(\alpha_i)\Big)=ct+\sum_{i=1}^r c_i l\circ\sigma(\varepsilon_i),\ 0\leqslant c_i<1\Big\},$$

这是 $\mathbb{R}^n$ 中一个形状良好的集合. 而由(4)式知 $w_K f(C, x)$ 不过是集合 $(xN(\mathfrak{B}))^{\frac{1}{n}}\Gamma_0$ 中整点 $(x_1, \cdots, x_n)$ 的个数. 当 $x\to\infty$ 时, $(xN(\mathfrak{B}))^{\frac{1}{n}}\Gamma_0$ 中整点个数相当于集合 $(xN(\mathfrak{B}))^{\frac{1}{n}}\Gamma_0$ 的体积

$$V((xN(\mathfrak{B}))^{\frac{1}{n}}\Gamma_0)=xN(\mathfrak{B})V(\Gamma_0)$$

的大小(每单位体积有一个整点!),而误差的阶应当为 $(xN(\mathfrak{B}))^{\frac{1}{n}}\Gamma_0$ 的表面积的测度, 即误差的阶应当为 $O(x^{\frac{1}{n}(n-1)})=O(x^{1-\frac{1}{n}})$. 因此我们有

$$w_K f(C, x)=xN(\mathfrak{B})V(\Gamma_0)+O(x^{1-\frac{1}{n}}) \quad (x\to\infty\text{ 时}). \qquad (5)$$

第三步(计算 $V(\Gamma_0)$)令

$$\sum_{i=1}^n x_i\sigma(\alpha_i)=(y_1, \cdots, y_{r_1}, y_{r_1+1}+iy_{r_1+r_2+1}, \cdots, y_{r_1+r_2}+iy_n).$$

即
$$y_k=\sum_{j=1}^n x_j\sigma_k(\alpha_j) \quad (1\leqslant k\leqslant r_1),$$

$$y_k+iy_{r_2+k}=\sum_{j=1}^n x_j\sigma_k(\alpha_j) \quad (r_1+1\leqslant k\leqslant r_1+r_2),$$

则

$$
\Gamma_0=\left\{(y_1,\cdots,y_n)\in\mathbb{R}^n\;\middle|\;\begin{array}{l}
\text{(i)}\ 0<|y_1\cdots y_{r_1}(y_{r_1+1}^2+y_{r_1+r_2+1}^2)\cdots \\
\qquad (y_{r_1+r_2}^2+y_n^2)|\leqslant 1. \\
\text{(ii)}\ (\log|y_1|,\ \cdots,\ \log|y_{r_1}|, \\
\qquad \log(y_{r_1+1}^2+y_{r_1+r_2+1}^2),\ \cdots, \\
\qquad \log(y_{r_1+r_2}^2+y_n^2))=ct+\sum_{i=1}^{r}c_i l\circ\sigma(\varepsilon_i) \\
\qquad (0\leqslant c_i<1,\ c\in\mathbb{R}).
\end{array}\right\}
\tag{6}
$$

再令 $\Gamma=\{(y_1,\ \cdots,\ y_n)\in\Gamma_0\,|\,y_i>0(1\leqslant i\leqslant r_1)\}$，则

$$
\begin{aligned}
V(\Gamma_0)&=\int_{\Gamma_0}\mathrm{d}x_1\cdots\mathrm{d}x_n \\
&=2^{r_1}\int_{\Gamma}J\left(\frac{y_1,\ \cdots,\ y_n}{x_1,\ \cdots,\ x_n}\right)^{-1}\mathrm{d}y_1\cdots\mathrm{d}y_n.
\end{aligned}
\tag{7}
$$

由于
$$
\frac{\partial y_k}{\partial x_j}=\begin{cases}\sigma_k(\alpha_j),\ 1\leqslant k\leqslant r_1; \\ \mathrm{Re}(\sigma_k(\alpha_j)),\ r_1+1\leqslant k\leqslant r_1+r_2; \\ \mathrm{Im}(\sigma_k(\alpha_j)),\ r_1+r_2+1\leqslant k\leqslant n.\end{cases}
$$

即知 Jacobi 行列式为

$$
\begin{aligned}
J\left(\frac{y_1,\ \cdots,\ y_n}{x_1,\ \cdots,\ x_n}\right)&=2^{-r_2}|\det(\sigma_i(\alpha_j))|=2^{-r_2}d(\alpha_1,\ \cdots,\ \alpha_n)^{1/2} \\
&=2^{-r_2}N(\mathfrak{B})\,|d(K)|^{1/2}.
\end{aligned}
$$

从而由(7)式即知

$$
V(\Gamma_0)=\frac{2^{r_1+r_2}}{N(\mathfrak{B})\,|d(K)|^{1/2}}V(\Gamma).
\tag{8}
$$

为了计算 $V(\Gamma)$，我们在 $\mathbb{R}^n=\mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$ 中引入极坐标：

$$
\begin{aligned}
&\rho_i=y_i\quad(1\leqslant i\leqslant r_1), \\
&\rho_{r_1+j}(\cos\theta_j+i\sin\theta_j)=y_{r_1+j}+iy_{r_1+r_2+j}\quad(1\leqslant j\leqslant r_2).
\end{aligned}
$$

于是

$$
\Gamma=\left\{(\rho_1,\cdots,\rho_{r_1+r_2},\ \theta_1,\cdots,\theta_{r_2})\;\middle|\;\begin{array}{l}
\text{(i)}\ 0\leqslant P=\rho_1\cdots\rho_{r_1} \\
\qquad\cdot(\rho_{r_1+1}\cdots\rho_{r_1+r_2})^2\leqslant 1; \\
\text{(ii)}\ \log\rho_i=\dfrac{\log P}{n} \\
\qquad+\sum_{j=1}^{r}c_j\log|\varepsilon_j^{(i)}|,\ 0\leqslant c_j<1; \\
\text{(iii)}\ 0\leqslant\theta_j<2\pi(1\leqslant j\leqslant r_2).
\end{array}\right\}
$$

这里我们利用了 $c=\log P/n$（此式可由(6)式中条件(ii)得到）．不难看出

$$J\left(\frac{y_1, \cdots, y_n}{\rho_1, \cdots, \rho_{r_1+r_2}, \theta_1, \cdots, \theta_{r_2}}\right)=\rho_{r_1+1}\cdots\rho_{r_1+r_2}$$

从而

$$\begin{aligned}V(\Gamma)&=\int_{\rho,\theta}\rho_{r_1+1}\cdots\rho_{r_1+r_2}\mathrm{d}\rho_1\cdots\mathrm{d}\rho_{r_1+r_2}\mathrm{d}\theta_1\cdots\mathrm{d}\theta_{r_2}\\&=(2\pi)^{r_2}\int_{\rho}\rho_{r_1+1}\cdots\rho_{r_1+r_2}\mathrm{d}\rho_1\cdots\mathrm{d}\rho_{r_1+r_2},\end{aligned}$$

再将坐标 $(\rho_1, \cdots, \rho_{r_1+r_2})$ 改成 $(P, c_1, \cdots, c_r)$．由于

$$\frac{\partial\rho_i}{\partial P}=\frac{\rho_i\partial\log\rho_i}{\partial P}=\frac{\rho_i}{nP}\quad(1\leqslant i\leqslant r_1+r_2),$$

$$\frac{\partial\rho_i}{\partial c_j}=\frac{\rho_i\partial\log\rho_i}{\partial c_j}=\rho_i\cdot\log|\varepsilon_j^{(i)}|\quad(1\leqslant j\leqslant r),$$

从而

$$\begin{aligned}&J\left(\frac{\rho_1, \cdots, \rho_{r_1+r_2}}{P, c_1, \cdots, c_r}\right)\\&=\left|\det\begin{pmatrix}\frac{\rho_1}{nP}, \cdots, \frac{\rho_{r_1+r_2}}{nP}\\ \rho_1\log|\varepsilon_1^{(1)}|, \cdots, \rho_{r_1+r_2}\log|\varepsilon_1^{(r_1+r_2)}|\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \rho_1\log|\varepsilon_r^{(1)}|, \cdots, \rho_{r_1+r_2}\log|\varepsilon_r^{(r_1+r_2)}|\end{pmatrix}\right|\\&=\frac{\rho_1\cdots\rho_{r_1+r_2}}{nP\cdot 2^{r_2}}R_K\cdot n.\end{aligned}$$

从而

$$\begin{aligned}V(\Gamma)&=(2\pi)^{r_2}\int_{0\leqslant P, c_1, \cdots, c_r\leqslant 1}\rho_1\cdots\rho_{r_1}\rho_{r_1+1}^2\cdots\rho_{r_1+r_2}^2\\&\quad\cdot\frac{R_K\cdot n}{nP\cdot 2^{r_2}}\mathrm{d}P\mathrm{d}c_1\cdots\mathrm{d}c_r\\&=\pi^{r_2}R_K.\end{aligned}$$

将此与(5)，(8)二式放在一起，即得

$$f(c, x)=\frac{2^{r_1}(2\pi)^{r_2}R_K}{w_K|d(K)|^{1/2}}x+O(x^{1-\frac{1}{n}})\quad(x\to\infty).\quad\blacksquare$$

定理 14 $\zeta_K(C, s)$ 与 $\zeta_K(s)$ 均可解析延拓到半平面 $\mathrm{Re}(s)>1-\frac{1}{n}$ 中，并且它们仅在 $s=1$ 处有单极点，其留数分别为

$$\operatorname*{res}_{s=1}\zeta_K(C,\ s)=\rho_K,\quad \operatorname*{res}_{s=1}\zeta_K(s)=h_K\rho_K.$$

证明 根据定理 1, $\zeta_K(C,\ s)=\rho_K\zeta(s)+\sum\limits_{n=1}^{\infty}(a_n(C)-\rho_K)n^{-s}$. 而当 $N\to\infty$ 时,

$$\sum_{n=1}^{N}(a_n(C)-\rho_K)=f(C,\ N)-\rho_K N=O(N^{1-\frac{1}{n}}).$$

从而由 § 9 的定理 1, 可知 $\sum\limits_{n=1}^{\infty}(a_n(C)-\rho_K)n^{-s}$ 在 $\mathrm{Re}(s)>1-\dfrac{1}{n}$ 中正则. 而 $\zeta(s)$ 在 $s=1$ 有单极点, 从而

$$\operatorname*{res}_{s=1}\zeta_K(C,\ s)=\rho_K\operatorname*{res}_{s=1}\zeta(s)=\rho_K.$$

最后

$$\begin{aligned}\operatorname*{res}_{s=1}\zeta_K(s)&=\sum_{C\in C(K)}\operatorname*{res}_{s=1}\zeta_K(C,\ s)=\rho_K\sum_{C\in C(K)}1\\&=\rho_K|C(K)|=\rho_K h_K.\end{aligned}$$ ∎

至此我们把 $\zeta_K(C,\ s)$ 和 $\zeta_K(s)$ 解析延拓到 $\mathrm{Re}(s)>1-\dfrac{1}{n}$, 为了进一步延拓到整个复平面上, 我们也需要函数方程.

3.2 $\zeta_K(s)$ 的函数方程

定理 15

(a) $\zeta_K(s)=\sum\limits_{\mathfrak{a}}N(\mathfrak{a})^{-s}$ 可以解析延拓成整个复平面上的亚纯函数, 并且只有 $s=1$ 是奇点(而且是单极点, 留数为 $\rho_K h_K$).

(b) 令

$$\Phi(s)=\left(\frac{|d(K)|}{4^{r_2}\pi^n}\right)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s),$$

则有函数方程

$$\Phi(s)=W\cdot\Phi(1-s),$$

其中 W 为(依赖于 K 的)复常数, 并且 $|W|=1$.

证明大意 我们目前已经具备有证明此定理所需的全部知识和技巧. 但是计算过于复杂. 所以这里只扼要地介绍一下主要思想, 完整的证明可见 E. Hecke 著名的《代数数论讲义》一书(Vorlesungen über die Theorie der algebraischen Zahlen, 1923 年),

或者 E. Landau 的书"Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der Ideale"(1918 年, p. 55～77).

事实上, 对于每个理想类 $C\in C(K)$, 均可给出 $\zeta_K(C, s)$ 的解析延拓和函数方程. 然后合并起来就得到 $\zeta_K(s)$ 的结果. 对于 $\zeta_K(C, s)$, 首先象定理 3 证明的第一步那样, 将理想求和化为元素求和:

$$
\begin{aligned}
\zeta_K(C, s) &= \sum_{\mathfrak{a}\in C} N(\mathfrak{a})^{-s} = \sum_{\substack{\alpha\in\mathfrak{B}\\ \alpha(\bmod U_K)}} (N(\alpha)N(\mathfrak{B})^{-1})^{-s} \\
&= N(\mathfrak{B})^{s} \sum_{\substack{\alpha\in\mathfrak{B}\\ \alpha(\bmod U_K)}} N(\alpha)^{-s} \\
&= N(\mathfrak{B})^{s} \sum_{\substack{\alpha=x_1\alpha_1+\cdots+x_n\alpha_n(\bmod U_K)\\ x_i\in\mathbf{Z}}} \prod_{i=1}^{n} (x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)})^{-s} \\
&= N(\mathfrak{B})^{s} \sum_{\substack{x_1,\cdots,x_n=-\infty\\ \alpha(\bmod U_K)}}^{\infty} \prod_{i=1}^{r_1} (x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)})^{-s} \\
&\quad\cdot \prod_{i=r_1+1}^{r_1+r_2} |x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)}|^{-2s},
\end{aligned}
$$

其中 $\mathfrak{B}$ 为理想类 C^{-1} 中任意一个整理想, 而 $\alpha_1, \cdots, \alpha_n$ 为加法群 $\mathfrak{B}$ 的一组基. 随后象定理 3 证明第二步那样, 将 $\bmod U_K$ 条件用 Dirichlet 单位定理加以改造(详情从略). 再对于上式右边乘积中的每个因子, 象处理 $\zeta(s)$ 和 $L(s, \chi)$ 时一样借助于 Gamma 函数化为积分, 具体来说, 就是使用

$$
\begin{aligned}
&\pi^{-s/2}\Gamma(s/2)(x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)})^{-s} \\
&\quad= \int_0^\infty e^{-\pi(x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)})^2 t}\, t^{s/2-1}\,\mathrm{d}t \quad (1\leqslant i\leqslant r_1),
\end{aligned}
$$

$$
\begin{aligned}
&\pi^{-s}\Gamma(s)|x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)}|^{-2s} \\
&\quad= \int_0^\infty e^{-\pi|x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)}|^2 t}\, t^{s-1}\,\mathrm{d}t \quad (r_1+1\leqslant i\leqslant r_1+r_2),
\end{aligned}
$$

于是

$$\pi^{-\frac{ns}{2}}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\prod_{i=1}^{r_1}\left(x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)}\right)^{-s}$$

$$\cdot\prod_{i=1}^{r_2}\left|x_1\alpha_1^{(i)}+\cdots+x_n\alpha_n^{(i)}\right|^{-2s}$$

$$=\int_0^{\infty}\cdots\int_0^{\infty}\mathrm{d}t_1\cdots\mathrm{d}t_{r_1+r_2}(t_1\cdots t_{r_1})^{s/2-1}(t_{r_1+1}\cdots t_{r_1+r_2})^{s-1}$$

$$\cdot\sum_{x_1,\cdots,x_n=-\infty}^{\infty}e^{-\pi tQ(\bar{x})},$$

其中 $Q(\bar{x})=Q(x_1,\cdots,x_n)$ 为 $x_1,\cdots,x_n$ 的一个二次型. 令

$$\theta(Q,t)=\sum_{x_1,\cdots,x_n=-\infty}^{\infty}e^{-\pi tQ(\bar{x})}.$$

用高维的 Poisson 求和公式可得到

$$\theta(\tilde{Q},t^{-1})=C\cdot\theta(Q,t),$$

其中 C 是一个相当复杂的常数(主要成份是代数数域上的 Gauss 和), $\tilde{Q}$ 是与 Q 相联系的另一个二次型, $\tilde{Q}$ 和 Q 都是正定的二次型. 于是由积分公式将 $\zeta_K(s)$ 延拓到整个复平面上. 再利用 $\theta(Q,t)$ 的上述变换公式, 经过相当冗长的计算, 即得到定理中的函数方程. 其中常数 W 很复杂, 但是可以计算出它的绝对值是 1. ▌

利用函数方程我们又可得到 $\zeta_K(s)$ 的零点特性与极点特性. 与前面 $\zeta(K)$ 和 $L(s,\chi)$ 一样, 我们首先需要

引理 10 $\zeta_K(1+it)\neq 0\quad(t\in\mathbb{R})$.

证明 我们已经知道 $s=1$ 是 $\zeta_K(s)$ 的单极点. 而当 $t\neq 0$ 时, 证明 $\zeta_K(1+it)\neq 0$ 几乎与证明 $\zeta(1+it)\neq 0$ 完全一样, 只要把 §10 中引理 5 证明中的有理素数 p 均改成 $N(p)$ 即可. ▌

引理 11 (a) $\zeta_K(s)$ 只有 $s=1$ 为奇点, 并且是留数为 $\rho_K h_K$ 的单极点;

(b) $\zeta_K(s)$ 在 $s=0$ 为 $r=r_1+r_2-1$ 阶零点, 在 $s=-2,-4,-6,\cdots$ 处为 $r+1$ 阶零点, 在 $s=-1,-3,-5,\cdots$ 处为 r_2 阶零点(以上均称作是 $\zeta_K(s)$ 的平凡零点), 而 $\zeta_K(s)$ 的其他零点均在区域 $0<\mathrm{Re}(s)<1$ 之中, 并且关于直线 $\mathrm{Re}(s)=1/2$ 是对称的.

证明 利用定理 4 中的函数方程, Gamma 函数的极点特性以及引理 1 即可证得全部结论, 证明与对 $\zeta(s)$ 和 $L(s, \chi)$ 的作法完全一样. ∎

注记

(1) 猜想对于每个数域 K, $\zeta_K(s)$ 的非平凡零点均在直线 $\mathrm{Re}(s)=1/2$ 之上. 这是通常 Riemann 猜想(对 $K=\mathbb{Q}$ 的情形)的推广. 目前还没有一个数域 K (甚至 $\mathbb{Q}$) 能够解决这个猜想.

(2) 关于 $\zeta_K(s)$ 人们还有许多猜想. 其中著名的 Artin 猜想是说: 如果数域 K 是数域 L 的子域, 则 $\zeta_L(s)/\zeta_K(s)$ 是整个复平面上的全纯函数. 根据引理 2, $\zeta_L(s)$ 和 $\zeta_K(s)$ 的单极点 $s=1$ 相互抵消. 因此 Artin 猜想相当于说: $\zeta_K(s)$ 的每个零点均是 $\zeta_L(s)$ 的零点, 并且前者的阶数不超过后者的阶数. 从引理 2 又可看到, 对于平凡零点这个结论是对的(换句话说, 域 K 的 r 和 r_2 分别不超过域 L 的 r 和 r_2, 从 r 和 r_2 的定义很容易证出这一点 (习题)). 问题在于: 对于 $\zeta_L(s)$ 和 $\zeta_K(s)$ 在带状区域 $0<\mathrm{Re}(s)<1$ 中的那些神秘的非平凡零点, 是否也有同样的结论? 我们在本书最后一章中要证明, 当 L 和 K 均是 Abel 数域的时候 $(L\supseteq K)$, Artin 猜想是对的. 1946 年, Brauer 利用有限群表示理论证明了: 如果 L/K 是数域的 Galois 扩张, 则 Artin 猜想是对的. 对于一般情形至今仍未解决.

(3) 我们在 § 10 中计算出 $\zeta(s)$ 和 $L(s,\chi)$ 在 $s=0, -1, -2, \cdots$ 处的值. 当 K 为 Abel 数域时, 我们在第六章要给出 $\zeta_K(s)$ 在 $s=0, -1, -2, \cdots$ 处的值. 对于任意的代数数域 K, 近来人们有许多奇妙的猜想, 将 $\zeta_K(n)$, $n=0, -1, -2, \cdots$ 与某些微分流形的不变量联系起来, 或者与代数 K-理论中的某些 K-群 $K_n(O_K)$ 的结构发生关系. 这些猜想是代数数论与微分几何, 调和分析, 代数几何, 自守函数理论等许多学科相互交织的产物, 在当前是一个很活跃的领域. 对于全实的数域 K (即 $r_1=[K:\mathbb{Q}]$), 日本年青而早逝的数学家新谷(Shintani)于 1978 年给出了计算 $\zeta_K(n)$ $(n=0, -1, -2, \cdots)$ 的一个初等的公式. 但是对于一般的数域 K, 关于

$\zeta_K(s)$取值方面的研究还有许多空白.

(4) 至于$\zeta_K(s)$在正整数处的取值, 最值得注意的是$\zeta_K(s)$在$s=1$的留数与域K的类数h_K相联系: $\underset{s=1}{\mathrm{res}}\,\zeta_K(s)=\rho_K h_K$. 这就表明对$\zeta_K(s)$的解析性质的研究会给出类数问题的结果. 目前研究最为透彻的是 Abel 数域的情形. 是由 Hasse 和他的学生 Leopoldt 于本世纪四十年代至六十年代作出的. 其中最基本结果是 Hasse 对于 Abel 数域的类数解析公式. 这是我们在第六章中要介绍的主题.

习　题

1. 设L/K是数域的扩张. 求证$r(L)\geqslant r(K)$, $r_2(L)\geqslant r_2(K)$. 其中$r(L)$和$r_2(L)$分别表示数域L的不变量$r=r_1+r_2-1$和r_2.

2. 对于数域K中每个整理想$\mathfrak{a}$, 定义

$$\varphi(\mathfrak{a})=|(O_K/\mathfrak{a})^*|,$$

$$d_m(\mathfrak{a})=\prod_{\mathfrak{B}|\mathfrak{a}}N(\mathfrak{B})^m\quad(\text{其中}\ \mathfrak{B}\ \text{过}\ \mathfrak{a}\ \text{的整理想因子}),$$

$$\bar{d}_m(\mathfrak{a})=\mathfrak{a}\ \text{分解成}\ m\ \text{个整理想之积的方法数}$$

(因子次序不同看作是不同的分解),

$$\mu(\mathfrak{a})=\begin{cases}1, & \text{若}\ \mathfrak{a}=O_K;\\ (-1)^r, & \text{若}\ \mathfrak{a}\ \text{为}\ r\ \text{个不同素理想之乘积};\\ 0, & \text{否则}.\end{cases}$$

求证:

(a) $\sum_{\mathfrak{a}}\mu(\mathfrak{a})N(\mathfrak{a})^{-s}=\zeta_K(s)^{-1}$, $\sum_{\mathfrak{a}}\bar{d}_m(\mathfrak{a})N(\mathfrak{a})^{-s}=\zeta_K(s)^m$,

$\sum_{\mathfrak{a}}d_m(\mathfrak{a})N(\mathfrak{a})^{-s}=\zeta_K(s)\zeta_K(s-m)$,

$\sum_{\mathfrak{a}}\varphi(\mathfrak{a})N(\mathfrak{a})^{-s}=\zeta_K(s-1)/\zeta_K(s)$;

(b) $\sum_{\mathfrak{B}|\mathfrak{a}}\varphi(\mathfrak{B})=N(\mathfrak{a})$, $\sum_{\mathfrak{B}|\mathfrak{a}}\dfrac{\mu(\mathfrak{B})}{N(\mathfrak{B})}=\dfrac{\varphi(\mathfrak{a})}{N(\mathfrak{a})}$.

3. 对于数域K中每个整理想$\mathfrak{a}$, 定义

$$\Lambda_K(\mathfrak{a})=\begin{cases}\log N(\mathfrak{p}), & \text{如果}\ \mathfrak{a}=\mathfrak{p}^m,\ m\geqslant 1,\ \mathfrak{p}\ \text{为素理想};\\ 0, & \text{否则}.\end{cases}$$

求证当 $\mathrm{Re}(s)>1$ 时

$$\sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a})N(\mathfrak{a})^{-s}=-\zeta_K'(s)/\zeta_K(s),$$

其中 ζ_K' 表示函数 $\zeta_K(s)$ 的导函数，特别对于通常的 Mongoldt 函数 $\Lambda(n)$，我们有 $\sum_{n=1}^{\infty}\Lambda(n)n^{-s}=-\zeta'(s)/\zeta(s)\qquad(\mathrm{Re}(s)>1)$。

第五章 密度问题

这一章里我们准备研究这样的问题：在每个数域 K 中，范不超过 x 的素理想（或者更一般地，具有某种性质的素理想）有多少个？对于 $K=\mathbb{Q}$ 的情形，这就是古典数论里的素数问题. 我们在本书引言中已经简略地谈到素数问题的历史. 如果我们定义数论函数

$$f(n)=\begin{cases}1, & \text{若 } n \text{ 为素数;}\\ 0, & \text{否则.}\end{cases}$$

那末它的部分和

$$\pi(x)=\sum_{n\leqslant x}f(n)=\sum_{p\leqslant x}1$$

恰好是不超过 x 的素数的个数. 公元前三世纪欧几里德证明了素数有无限多个，这可以表示成 $\pi(x)\to+\infty$（当 $x\to+\infty$）时. 后来，采用古典的 Eratosthenes 筛法证明了

$$\lim_{x\to\infty}\frac{\pi(x)}{x}=0.$$

由于不超过 x 的整数共有 $[x]$ 个，因此这个结果意味着素数在整数中是稀疏的，这就涉及到素数的密度问题. 十八至十九世纪，Legendre 和 Gauss 等人基于大量的计算结果（手算！），猜想 $\lim\limits_{x\to\infty}\pi(x)/(x/\log x)=1$（这里 $\log x$ 和在本书中其他地方一样，均指是自然对数），在 Riemann 和 Dirichlet 引入解析工具之后，运用相当深刻的整函数理论，两个法国数学家 J. Hadamard 和 C. J. de la Vallée Poussin 于 1896 年各自独立地证明了素数定理，即 $\lim\limits_{x\to\infty}\pi(x)/(x/\log x)=1$. 1949 年，又有两个数学家 A. Selberg 和 P. Erdös 独立地给出素数定理的初等证明（即不用复变函数理论的证明）.

另一方面，为了研究算术级数中的素数分布，Dirichlet 发明

了我们在前章中介绍的 L-函数 $L(s,\chi)$，采用上面的解析方法，平行地证明了算术级数中的素数定理：令 $\pi(x;l,k)=\sum\limits_{\substack{p\leq x\\ p\equiv l(\bmod k)}}1$（其中 $(l,k)=1$），则 $\lim\limits_{x\to\infty}\dfrac{\pi(x;l,k)\log x}{x}=1/\varphi(k)$。同样地，1920 年德国数学家 Landau 利用 Dedekind zeta 函数 $\zeta_K(s)$ 和同样的解析手段，证明了代数数域中的素理想定理：对于每个数域 K，令 $\pi_K(x)=\sum\limits_{\substack{\mathfrak{p}\\ N(\mathfrak{p})\leq x}}1$，即 K 中范不超过 x 的素理想个数，则

$$\lim_{x\to+\infty}\pi_K(x)/(x/\log x)=1.$$

我们在本章中首先给大家介绍年青数学家 D. Zagier 于 1982 年访华期间所介绍的关于素数定理的一个简单证明。然后我们说明这个办法也可以证明算术级数中的素数定理和素理想定理，这是 § 12 的内容。在 § 13 中我们要介绍具有某种性质的素理想的密度定理，并且应用它来研究多项式在有限域中的分解特性。

§ 1 素数定理和素理想定理

1.1 素数定理

如上所述，令

$$f(n)=\begin{cases}1, & \text{若 } n \text{ 为素数；}\\ 0, & \text{否则.}\end{cases}$$

$$\pi(x)=\sum_{n\leq x}f(n)=\sum_{p\leq x}1.$$

根据 Dirichlet 级数的一般理论，$\pi(x)$ 的大小应当与 D-级数

$$\sum_{n=1}^{\infty}f(n)n^{-s}=\sum_{p}p^{-s}$$

有直接关系。遗憾的是，这个 D-级数不能象许多数论函数的 D-级数那样可以用 $\zeta(s)$ 等熟知的函数直接表达出来，所以作为第一步，我们要将对 $\pi(x)$ 的研究归结于另一个数论函数的研究，使得后者的 D-级数是熟知的。这个新的数论函数就是我们已经介绍过的 Von Mangoldt 函数：

$$\Lambda(n)=\begin{cases}\log p, & 若\ n=p^r,\ r\geqslant 1,\ p\ 为素数;\\ 0, & 否则.\end{cases}$$

当 $\operatorname{Re}(s)>1$ 时，由于 $\zeta'(s)=-\sum_{n=1}^{\infty}\log n\cdot n^{-s}$ 和公式 $\sum_{d\mid n}\Lambda(d)=\log n$（§9 习题 2），从而在数论函数环中，$\{\Lambda(n)\}*\{1\}=\{\log n\}$. 因此 $\zeta'(s)=-\zeta(s)\sum_{n=1}^{\infty}\Lambda(n)n^{-s}$. 从而作为复变函数，我们有

$$-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}\Lambda(n)n^{-s}\quad(\operatorname{Re}(s)>1).$$

又令 $\psi(x)=\sum_{n\leqslant x}\Lambda(n)$ 是函数 $\Lambda(n)$ 的部分和，则当 $\operatorname{Re}(s)>1$ 时

$$\int_1^{\infty}\frac{\psi(t)\,\mathrm{d}t}{t^{s+1}}=\int_1^{\infty}\sum_{n\leqslant t}\Lambda(n)\frac{\mathrm{d}t}{t^{s+1}}=\sum_{n=1}^{\infty}\Lambda(n)\int_n^{\infty}\frac{\mathrm{d}t}{t^{s+1}}$$
$$=s^{-1}\sum_{n=1}^{\infty}\Lambda(n)n^{-s}.$$

从而我们得到

$$-\frac{\zeta'(s)}{\zeta(s)}=s\int_1^{\infty}\frac{\psi(t)\,\mathrm{d}t}{t^{s+1}}\quad(\operatorname{Re}(s)>1),\tag{1}$$

而下面引理将素数定理归结为对 $\psi(x)$ 的估计.

引理 1 如果 $\lim_{x\to\infty}\frac{\psi(x)}{x}=1$，则 $\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1$.

证明 首先我们有

$$\psi(x)=\sum_{n\leqslant x}\Lambda(n)=\sum_{p^m\leqslant x}\log p\leqslant\sum_{p\leqslant x}\frac{\log x}{\log p}\log p=\pi(x)\log x,\tag{2}$$

从而 $\underline{\lim}_{x\to\infty}\frac{\pi(x)\log x}{x}\geqslant\lim_{x\to\infty}\frac{\psi(x)}{x}=1$. 另一方面，对于每个 $0<\alpha<1$ 和 $x>1$，均有

$$\psi(x)\geqslant\sum_{x^{\alpha}<p\leqslant x}\log p\geqslant\{\pi(x)-\pi(x^{\alpha})\}\log(x^{\alpha})$$
$$\geqslant\alpha(\pi(x)-x^{\alpha})\log x,$$

从而 $\quad\overline{\lim}_{x\to\infty}\frac{\pi(x)\log x}{x}\leqslant\frac{1}{\alpha}\lim_{x\to\infty}\frac{\psi(x)}{x}+\lim_{x\to\infty}\frac{x^{\alpha}\log x}{x}=\frac{1}{\alpha}$.

令 $\alpha\to 1$，于是 $\overline{\lim}_{x\to\infty}\frac{\pi(x)\log x}{x}\leqslant 1$. 两者合并即得到

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1. \qquad \blacksquare$$

注记 由 $\lim\limits_{x\to\infty}\frac{\pi(x)\log x}{x}=1$ 也可以推出 $\lim\limits_{x\to\infty}\frac{\psi(x)}{x}=1$，不过今后我们不需要这一事实.

引理 1 将问题化为证明 $\lim\limits_{x\to\infty}\frac{\psi(x)}{x}=1$. 现在再作进一步的转化.

引理 2 若 $\int_1^\infty\frac{\psi(t)-t}{t^2}\,dt$ 收敛，则 $\lim\limits_{x\to\infty}\frac{\psi(x)}{x}=1$.

证明 用反证法. 如果 $\frac{\psi(x)}{x}$ 不以 1 为极限，则或者存在 $c>1$ 和序列 $x_n\to+\infty$，使得 $\psi(x_n)\geqslant cx_n(n=1,2,\cdots)$ 或者存在 $0<c<1$, $x_n\to+\infty$，使得 $\psi(x_n)\leqslant cx_n(n=1,2,\cdots)$. 对于第一种情形，由于 $\psi(x)$ 为递增函数，从而

$$\int_{x_n}^{cx_n}\frac{\psi(t)-t}{t^2}\,dt\geqslant\int_{x_n}^{cx_n}\frac{cx_n-t}{t^2}\,dt=(c-1)-\log c>0$$

$$(n=1,2,\cdots).$$

这就与 $\int_1^\infty\frac{\psi(t)-t}{t^2}\,dt$ 收敛相矛盾. 类似地，对于第二种情形，

$$\int_{cx_n}^{x_n}\frac{\psi(t)-t}{t^2}\,dt\leqslant\int_{cx_n}^{x_n}\frac{cx_n-t}{t^2}\,dt=1-c+\log c<0$$

$$(n=1,2,\cdots),$$

又与 $\int_1^\infty\frac{\psi(t)-t}{t^2}\,dt$ 收敛相矛盾. $\blacksquare$

于是问题又化为证明 $\int_1^\infty\frac{\psi(t)-t}{t^2}\,dt$ 收敛. 为了证明这一点，我们需要如下最关键的引理.

分析引理 假设 $f(t)$ 为实变函数，并且

(a) 当 $t\geqslant1$ 时，$|f(t)|\leqslant M/t$；

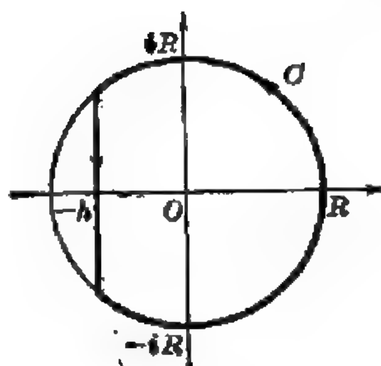
(b) $\tilde{g}(s)=\int_1^\infty\frac{f(t)}{t^s}\,dt\,(\mathrm{Re}(s)>0)$ 可以解析延拓成 $\mathrm{Re}(s)\geqslant0$ 上的正则函数 $g(s)$，则积分 $\int_1^\infty f(t)\,dt$ 收敛并且等于 $g(0)$.

证明 对于 $x\geqslant1$，定义 $g_x(s)=\int_1^x f(t)t^{-s}\,dt$. 我们只要证明当

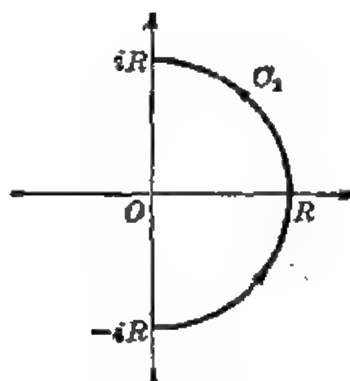
$x\to\infty$ 时，$g_x(0)\to g(0)$ 即可.

由于 $g_x(s)$ 是整个复平面上的全纯函数，而 $g(s)$ 在 $\operatorname{Re}(s)\geqslant 0$ 中正则，从而对每个点 $s=i\tau$，$g(s)$ 都在 $s=i\tau$ 的某个小邻域中正则. 因此对于给定的 $R>0$，存在某个充分小的 $h>0$，使得 $\frac{1}{s}(g_x(s)-g(s))$ 在图(一)所示的围道 C 中只有 $s=0$ 可能为极点. 于是由 Cauchy 积分定理我们有

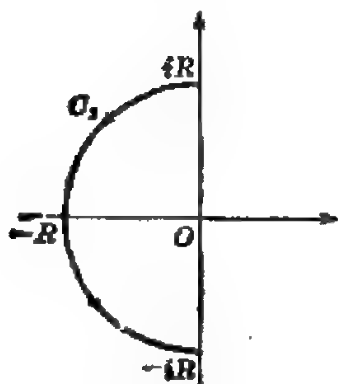
$$
\begin{aligned}
g_x(0)-g(0)&=\frac{1}{2\pi i}\int_C\frac{1}{s}(g_x(s)-g(s))x^s\cdot\left(\frac{s^2}{R^2}+1\right)ds\\
&=\frac{1}{2\pi i}\left(\int_{C_1}(g_x(s)-g(s))x^s\cdot\frac{s^2+R^2}{sR^2}ds\right.\\
&\quad+\int_{C_2}g_x(s)x^s\frac{s^2+R^2}{sR^2}ds\\
&\quad\left.-\int_{C_3}g(s)x^s\frac{s^2+R^2}{sR^2}ds\right)\\
&=\frac{1}{2\pi i}(\mathrm{I}+\mathrm{II}-\mathrm{III}),
\end{aligned}
$$



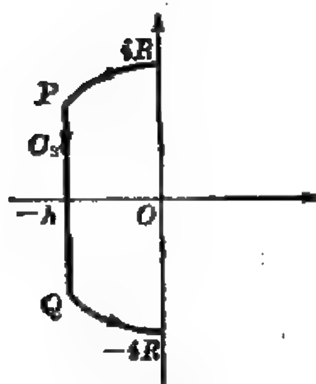
图(一)



图(二)



图(三)



图(四)

其中积分曲线 C_1, C_2 和 C_3 分别如图(二)、(三)、(四)所示.

对于 III 在 C_3 的两段弧上, $|x^s|\leqslant 1$, $\left|\frac{s^2+R^2}{sR^2}\right|\leqslant\frac{2}{R}$, 而 $|g(s)|$ 是有界的. 假设 $|g(s)|\leqslant N$, 则在这两段弧上被积函数的绝对值 $\leqslant 2\frac{N}{R}$. 而弧长为 $R\cdot\sin\frac{h}{R}\sim h$(当 $h/R\to 0$ 时). 从而这两段弧上的积分贡献为 $O(h/R)$, 于是若取充分小的 h 和充分大的 R, 可使两段弧上的积分任意小. 另一方面, 在 C_3 的直线段 $\overrightarrow{PQ}$ 上, $\mathrm{Re}(s)=-h$, 于是 $\overrightarrow{PQ}$ 上积分的绝对值 $\leqslant\int_{-h-R_i}^{-h+R_i}\left|\frac{g(s)}{s}\left(1+\frac{s^2}{R^2}\right)\right|\cdot x^{-h}|\mathrm{d}s|\leqslant Nx^{-h}\int_{-R}^{R}\frac{\mathrm{d}t}{\sqrt{h^2+t^2}}\leqslant 2Nx^{-h}\int_0^{R/h}\frac{\mathrm{d}y}{\sqrt{1+y^2}}$ (对于某常数 N). 从而在取定 h, R 之后而使 $x\to\infty$ 时, 可使 $|\mathrm{III}|$ 任意小.

对于 I 在 C_1 上当 $\sigma=\mathrm{Re}(s)>0$ 时, $g(s)=\tilde{g}(s)$, $|x^s|=|x^\sigma|$, $\left|\frac{s^2+R^2}{sR^2}\right|=\frac{2\sigma}{R^2}$. 由假设条件 $|f(t)|\leqslant M/t$, 从而

$$|g_x(s)-g(s)|=\left|\int_x^\infty\frac{f(t)}{t^s}\mathrm{d}t\right|\leqslant\int_x^\infty\frac{M}{t^{\sigma+1}}\mathrm{d}t=\frac{M}{\sigma}x^{-\sigma}.$$

因此 $$\left|x^s(g_x(s)-g(s))\frac{s^2+R^2}{sR^2}\right|\leqslant x^\sigma\cdot\frac{M}{\sigma}x^{-\sigma}\cdot\frac{2\sigma}{R^2}=\frac{2M}{R^2}.$$

取极限可知这对 $s=\pm iR$ 也对.

对于 II 在 C_2 上, 当 $\sigma=\mathrm{Re}(s)<0$ 时, $|x^s|=x^\sigma$, $|g_x(s)|=\left|\int_1^x\frac{f(t)}{t^s}\mathrm{d}t\right|\leqslant\int_1^x\frac{M\,\mathrm{d}t}{t^{\sigma+1}}\leqslant-\frac{M}{\sigma}x^{-\sigma}$, 从而

$$\left|x^s g_x(s)\frac{s^2+R^2}{sR^2}\right|\leqslant x^\sigma\cdot\frac{M}{\sigma}\cdot x^{-\sigma}\cdot\frac{2\sigma}{R^2}=\frac{2M}{R^2}.$$

取极限可知当 $s=\pm iR$ 时这也是对的. 于是

$$|\mathrm{I}+\mathrm{II}|\leqslant\int_{|s|=R}\frac{2M}{R^2}|\mathrm{d}s|=\frac{4\pi M}{R}\to 0\quad(\text{当 }R\to\infty\text{ 时}).$$

这就证明了分析引理. ▮

现在为了证明 $\int_1^\infty\frac{\psi(t)-t}{t^2}\mathrm{d}t$ 收敛. 我们在分析引理中取 $f(t)=\frac{\psi(t)-t}{t^2}$. 则分析引理中的条件(a)相当于

$$\psi(t)=O(t)\quad（当\ t\geqslant 1\ 时）. \tag{*}$$

而条件 (b) 相当于要求 $g(s)=\int_1^\infty \frac{f(t)}{t^s}\mathrm{d}t$ 可解析延拓成 $\mathrm{Re}(s)\geqslant 0$ 上的正则函数．但是由 (1) 式知当 $\mathrm{Re}(s)>0$ 时

$$g(s)=\int_1^\infty \frac{\psi(t)}{t^{s+2}}\mathrm{d}t-\int_1^\infty \frac{\mathrm{d}t}{t^{s+1}}=-\frac{1}{s+1}\frac{\zeta'(s+1)}{\zeta(s+1)}-\frac{1}{s}.$$

根据 $\zeta(s)$ 的性质，上式右边在 $\mathrm{Re}(s)\geqslant 0$ 内只可能在 $s=0$ 处有极点．但是在 $s=0$ 处，

$$-\frac{1}{s+1}\frac{\zeta'(s+1)}{\zeta(s+1)}-\frac{1}{s}\sim-\left(\log\frac{1}{s}\right)'-\frac{1}{s}=0.$$

从而在 $s=0$ 处也无极点．因此条件 (b) 是成立的．所以只需再证上面的 (*) 式成立，就由分析引理推得 $\int_1^\infty f(t)\mathrm{d}t=\int_1^\infty \frac{\psi(t)-t}{t^2}\mathrm{d}t$ 收敛，从而也就证明了素数定理． 注意 (*) 式 $\psi(t)=O(t)$ 比我们要证的 $\psi(t)\sim t\,(t\to+\infty$ 时) 弱很多，所以可以用很初等的方法证明它．

引理 3　当 $x\to+\infty$ 时，$\psi(x)=O(x)$．

证明　我们有

$$n^{\pi(2n)-\pi(n)}<\prod_{n<p<2n}p\leqslant\binom{2n}{n}\leqslant(1+1)^{2n}=4^n.$$

从而 $\pi(2n)-\pi(n)\leqslant\frac{n}{\log n}\cdot\log 4$． 特别地有 $\pi(2^{k+1})-\pi(2^k)\leqslant\frac{2^{k+1}}{k}$．但是易知 $\pi(2^{k+1})\leqslant 2^k$，从而

$$\begin{aligned}(k+1)\pi(2^{k+1})-k\pi(2^k)&\leqslant\pi(2^{k+1})+k(\pi(2^{k+1})-\pi(2^k))\\&\leqslant 2^k+2^{k+1}=3\cdot 2^k.\end{aligned}$$

在上式中取 $k=0,\ 1,\ 2,\ \cdots,\ l$，然后相加，即得到

$$(l+1)\pi(2^{l+1})\leqslant 3(1+2+2^2+\cdots+2^l)\leqslant 3\cdot 2^{l+1}.$$

即 $\pi(2^{l+1})<\frac{3\cdot 2^{l+1}}{l+1}$．对于任意的 $x\geqslant 2$，令 $2^l\leqslant x<2^{l+1}$，则

$$\pi(x)<\pi(2^{l+1})<\frac{3\cdot 2^{l+1}}{l+1}\leqslant\frac{6x}{\log x/\log 2}=x(\log 64)/\log x.$$

再由引理 1 证明中的 (2) 式即得到 $\psi(x)\leqslant(\log 64)x$．∎

至此我们就完全地证明了素数定理.

1.2 算术级数中的素数定理

Dirichlet 发明 L 函数是为了证明如下的算术级数中的素数定理.

定理 1 设 $(l, k)=1$, $k\geqslant 1$, $\pi(x; k, l)=\sum\limits_{\substack{p<x\\ p\equiv l(\bmod k)}} 1$. 则当 $x\to +\infty$ 时, $\pi(x; k, l)\sim\dfrac{x}{\varphi(k)\log x}$. 换句话说, 对于固定的正整数 k, 全体素数平均分布在 $\varphi(k)$ 个算术级数 $l+k\mathbb{Z}((l, k)=1)$ 之中. 特别地, 对于 $(l, k)=1$, 每个算术级数 $kn+l(n=1, 2, \cdots)$ 均包含无限多个素数.

证明 我们仍采用上述方法. 令

$$\psi(x, k, l)=\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n),\quad \psi(x, \chi)=\sum_{n\leqslant x}\chi(n)\Lambda(n).$$

其中 χ 为模 k 的 D-特征. 由特征正交关系可知

$$\psi(x, k, l)=\frac{1}{\varphi(k)}\sum_{\chi}\overline{\chi}(l)\psi(x, \chi).$$

(χ 过模 k 全部 D-特征).

与 $\zeta(s)$ 的情形一样地可以证得

$$-\frac{L'(s, \chi)}{L(s, \chi)}=\sum_{n=1}^{\infty}\Lambda(n)\chi(n)n^{-s}\quad (\mathrm{Re}(s)>1\text{ 时}).$$

从而可以得到类似于上小节中 (1) 式的:

$$-\frac{1}{\varphi(k)}\sum_{\chi}\overline{\chi}(l)\cdot\frac{L'(s, \chi)}{L(s, \chi)}=s\int_1^{\infty}\frac{\psi(t, k, l)}{t^{s+1}}\,\mathrm{d}t\quad (\mathrm{Re}(s)>1) \tag{1}$$

与引理 1 和引理 2 完全一样地可以证明:

引理 1′ 如果 $\lim\limits_{x\to\infty}\dfrac{\psi(x, k, l)\varphi(k)}{x}=1$, 则定理 2 成立. ▮

引理 2′ 若 $\displaystyle\int_1^{\infty}\frac{\psi(x, k, l)\varphi(k)-t}{t^2}\,\mathrm{d}t$ 收敛, 则

$$\lim_{x\to+\infty}\frac{\psi(x, k, l)\varphi(k)}{x}=1.\qquad ▮$$

又由引理 3 直接推出

引理 3' $\psi(x, k, l)=O(x)$ ($x\to+\infty$ 时).

于是在分析引理中取 $f(t)=\dfrac{\varphi(k)\psi(t, k, l)-t}{t^2}$. 由引理 3' 可知分析引理中的条件(a)成立. 另一方面, 当 $\mathrm{Re}(s)>0$ 时, 由 (1)' 式得到

$$g(s)=\int_1^\infty \frac{f(t)}{t^s}\,\mathrm{d}t=\int_1^\infty \frac{\varphi(k)\psi(t, k, l)}{t^{s+2}}\,\mathrm{d}t-\int_1^\infty \frac{\mathrm{d}t}{t^{s+1}}$$
$$=-\frac{1}{s+1}\sum_\chi \overline{\chi}(l)\,\frac{L'(s+1, \chi)}{L(s+1, \chi)}-\frac{1}{s}.$$

我们在前章中已经证明了 $L(s, \chi)$ 在 $\mathrm{Re}(s)\geqslant 1$ 中没有零点, 并且只在 $\chi=\chi_0$ 时有一个一阶极点 $s=1$. 设其留数为 A, 于是上式右边在 $\mathrm{Re}(s)\geqslant 0$ 中的奇性只可能于 $s=0$ 处. 可是当 $s=0$ 时,

$$-\frac{1}{s+1}\sum_\chi \overline{\chi}(l)\,\frac{L'(s+1, \chi)}{L(s+1, \chi)}-\frac{1}{s}\sim-\left(\log\frac{A}{s}\right)'-\frac{1}{s}=0.$$

从而 $g(s)$ 可解析延拓成 $\mathrm{Re}(s)\geqslant 0$ 上的正则函数, 于是条件(b)也成立. 因此由分析引理推出积分

$$\int_1^\infty f(t)\,\mathrm{d}t=\int_1^\infty \frac{\psi(t, k, l)\varphi(k)-t}{t^2}\,\mathrm{d}t$$

收敛. 再由引理 1' 和引理 2' 即证得定理 2. ∎

1.3 素理想定理

素理想定理是素数定理的平行推广, 是由 Landau 于 1920 年证明的. 设 K 是数域, 令

$$\pi_K(x)=\sum_{\substack{\mathfrak{p}\\ N(\mathfrak{p})\leqslant x}} 1 \quad (\mathfrak{p}\text{ 过 } O_K \text{ 中范不超过 } x \text{ 的所有素理想}).$$

定理 2(Landau, 素理想定理). $\pi_K(x)\sim\dfrac{x}{\log x}$ (当 $x\to+\infty$ 时).

证明 我们仍沿用上述方法. 对于 O_K 中每个非零整理想 $\mathfrak{a}$, 定义

$$\Lambda_K(\mathfrak{a})=\begin{cases}\log N(\mathfrak{p}), & \text{如果 } \mathfrak{a}=\mathfrak{p}^n,\ n\geqslant 1;\\ 0, & \text{否则},\end{cases}$$

$$\psi_K(x)=\sum_{N(\mathfrak{a})\leqslant x}\Lambda_K(\mathfrak{a})=\sum_{n\leqslant x}\Lambda_K(n),\quad \Lambda_K(n)=\sum_{N(\mathfrak{a})=n}\Lambda_K(\mathfrak{a}),$$

则当 $\mathrm{Re}(s)>1$ 时，$\log\zeta_K(s)=-\log\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})$，从而

$$-\frac{\zeta'_K(s)}{\zeta_K(s)}=\sum_{\mathfrak{p}}\frac{N(\mathfrak{p})^{-s}\log N(\mathfrak{p})}{1-N(\mathfrak{p})^{-s}}=\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}N(\mathfrak{p})^{-ms}\log N(\mathfrak{p})$$

$$=\sum_{\mathfrak{a}}\Lambda_K(\mathfrak{a})N(\mathfrak{a})^{-s}=\sum_{n=1}^{\infty}\Lambda_K(n)n^{-s}.$$

于是又可如前一样证得

$$s\int_1^{\infty}\frac{\psi_K(t)\,\mathrm{d}t}{t^{s+1}}=-\frac{\zeta'_K(s)}{\zeta_K(s)}\quad(\mathrm{Re}(s)>1).\qquad(1)''$$

引理 1″ 若 $\lim\limits_{x\to\infty}\frac{\psi_K(x)}{x}=1$，则 $\lim\limits_{x\to\infty}\frac{\pi_K(x)\log x}{x}=1$。

证明 与引理 1 的证明一样，由于

$$\psi_K(x)\leqslant\sum_{N(\mathfrak{p})\leqslant x}\frac{\log x}{\log N(\mathfrak{p})}\log N(\mathfrak{p})=\pi_K(x)\log x,\qquad(2)''$$

可知 $\varliminf\limits_{x\to\infty}\frac{\pi_K(x)\log x}{x}\geqslant\lim\limits_{x\to\infty}\frac{\psi_K(x)}{x}=1$。另一方面，对于 $0<\alpha<1$，我们有

$$\psi_K(x)\geqslant\sum_{x^\alpha<N(\mathfrak{p})\leqslant x}\log N(\mathfrak{p})\geqslant\{\pi_K(x)-\pi_K(x^\alpha)\}\log(x^\alpha)$$

$$\geqslant\alpha\pi_K(x)\cdot\log x-\alpha\cdot nx^\alpha\cdot\log x,\qquad n=[K:\mathbb{Q}].$$

(这里我们利用了 $\pi_K(x^\alpha)=\sum\limits_{N(\mathfrak{p})\leqslant x^\alpha}1\leqslant\sum\limits_{p\leqslant x^\alpha}\sum\limits_{\mathfrak{p}\mid p}1\leqslant n\sum\limits_{p\leqslant x^\alpha}\cdot 1\leqslant n\cdot x^\alpha$。)

从而

$$\varlimsup_{x\to\infty}\frac{\pi_K(x)\log x}{x}\leqslant\frac{1}{\alpha}\lim_{x\to\infty}\frac{\psi_K(x)}{x}+\lim_{x\to\infty}\frac{nx^\alpha\log x}{x}=\frac{1}{\alpha}.$$

令 $\alpha\to1$ 即得 $\varlimsup\limits_{x\to\infty}\frac{\pi_K(x)\log x}{x}\leqslant1$。两者合并即得 $\lim\limits_{x\to\infty}\frac{\pi_K(x)\log x}{x}=1$。 ▮

引理 2″ 若 $\int_1^{\infty}\frac{\psi_K(t)-t}{t^2}\mathrm{d}t$ 收敛，则 $\lim\limits_{x\to\infty}\frac{\psi_K(t)}{t}=1$。 ▮

引理 3″ 当 $x\to+\infty$ 时，$\psi_K(x)=O(x)$。

证明 因为 $\pi_K(x)\leqslant n\pi(x)\leqslant n\cdot\log64\cdot\frac{x}{\log x}$。再由(2)″式即得证。 ▮

现在于分析引理中取$f(t)=\frac{\psi_K(t)-t}{t^2}$. 由引理3″知条件(a)成立. 而由(1)″式知

$$g(s)=\int_1^\infty \frac{f(t)}{t^s}\mathrm{d}t=\int_1^\infty \frac{\psi_K(t)}{t^{s+2}}\mathrm{d}t-\int_1^\infty \frac{\mathrm{d}t}{t^{s+1}}$$
$$=-\frac{1}{s+1}\cdot\frac{\zeta'_K(s+1)}{\zeta_K(s+1)}-\frac{1}{s}.$$

我们在上节中已经证明了$\zeta_K(s)$在$\mathrm{Re}(s)\geqslant 1$中无零点, 并且只有$s=1$为单极点. 由此可知上式右边在$\mathrm{Re}(s)\geqslant 0$上无奇点, 于是$g(s)$可解析延拓到$\mathrm{Re}(s)\geqslant 0$. 于是条件(b)也成立. 由分析引理知$\int_1^\infty f(t)\mathrm{d}t=\int_1^\infty \frac{\psi_K(t)-t}{t^2}\mathrm{d}t$收敛. 再由引理1″和引理2″即证得素理想定理. ∎

§2 密度定理及其应用

2.1 Dirichlet 密度

我们现在讨论数域K中具有各种分解特性的素理想的密度问题. 我们也同时展示解析方法在研究素理想分解问题中所起的作用. 为此, 我们需要引进新的密度概念. 让我们从一个简单的例子——算术级数中的素数定理谈起.

设$(k, l)=1$. 如前面一样, 以$\pi(x, k, l)$表示算术级数$kn+l$ $(n=0, 1, 2, \cdots)$中不超过x的素数个数. 我们在§12中证明了: $\pi(x, k, l)\sim\frac{1}{\varphi(k)}\frac{x}{\log x}$ $(x\to+\infty$时). 特别地, 每个这样的算术级数中均有无限多个素数. 如果我们只想证明后面这一句话, 则有如下更为简单的方法.

对于每个模k的D-特征χ, 当$\mathrm{Re}(s)>1$时

$$\log L(s, \chi)=\sum_p \log(1-\chi(p)p^{-s})^{-1}=\sum_p\sum_{m=1}^\infty \frac{\chi(p)^m}{m}p^{-ms}$$
$$=\sum_p \chi(p)p^{-s}+g_\chi(s),$$

其中 $g_\chi(s)=\sum_p\sum_{m=2}^{\infty}\frac{\chi(p)^m}{m}p^{-ms}$. 易知 $g_\chi(s)$在 $\mathrm{Re}(s)>1/2$ 中收敛. 特别地, $g_\chi(s)$在 $s=1$ 处连续. 另一方面,

$$\sum_{p\equiv l(\mathrm{mod}\,k)}p^{-s}=\frac{1}{\varphi(k)}\sum_\chi\bar\chi(l)\sum_p\chi(p)p^{-s}$$
$$=\frac{1}{\varphi(k)}\sum_\chi\bar\chi(l)\log L(s,\chi)-\frac{1}{\varphi(k)}\sum_\chi\bar\chi(l)g_\chi(s).$$

如果 $\chi\neq\chi_0$, 则 $L(s,\chi)$在 $s=1$ 处正则. 而 $\log L(s,\chi_0)\sim\log\zeta(s)\sim-\log(s-1)$ (当 $s\to1^+$ 时). 此外, $\frac{1}{\varphi(k)}\sum_\chi\bar\chi(l)g_\chi(s)$在 $s=1$ 处正则. 于是

$$\sum_{p\equiv l(\mathrm{mod}\,k)}p^{-s}\sim\frac{1}{\varphi(k)}(-\log(s-1))\quad(\text{当 } s\to1^+ \text{ 时}).$$

由此式可知, 左边在 $s\to1^+$ 时应当趋于 $+\infty$. 因此对于每个 l, $(l,k)=1$, 算术级数 $kn+l(n\in\mathbb{Z})$中必存在无穷多个素数.

在这个证明过程的启示下, 我们现在给出

定义 1 设 K 是代数数域, A 是 K 的一个素理想集合. 如果 $\lim\limits_{s\to1^+}\sum\limits_{\mathfrak{p}\in A}N(\mathfrak{p})^{-s})/-\log(s-1)$ 存在, 则称此极限为素理想集合 A 的 Dirichlet 密度(简称作 D-密度), 并且记为 $\delta(A)$.

于是, 从上面定义前面的证明过程可知, 当$(l,k)=1$时, 对于算术级数 $l+k\mathbb{Z}$ 中的素数集合, 其 D-密度为 $1/\varphi(k)$. 不难看出, $\delta(A)$有如下一些简单性质: 设 A 和 A' 为某数域 K 的两个素理想集合, 则

(A) 如果 $A\subseteq A'$, 而 $\delta(A)$和 $\delta(A')$均存在, 则

$$\delta(A)\leqslant\delta(A').$$

(B) 如果 $\delta(A)$存在, 则 $0\leqslant\delta(A)\leqslant1$.

(C) 如果 $A\cap A'=\varnothing$ 而 $\delta(A)$和 $\delta(A')$均存在, 则 $\delta(A\cup A')$也存在, 并且 $\delta(A\cup A')=\delta(A)+\delta(A')$.

(D) 若 $|A|<+\infty$, 则 $\delta(A)=0$ (换句话说, 若 $\delta(A)>0$, 则 A 是无限集合).

下面的引理表明, 我们前面证明的素数定理和素理想定理比

关于D–密度方面的结果要强.

引理4 设 A 是数域 K 的一个素理想集合，令

$$\pi(x, A)=\sum_{\substack{\mathfrak{p}\in A\\ N(\mathfrak{p})\leqslant x}} 1,$$

如果 $\lim\limits_{x\to\infty}\dfrac{\pi(x, A)\log x}{x}=C_A$，则 $\delta(A)$ 存在并且等于 C_A.

证明 我们要证 $\sum\limits_{\mathfrak{p}\in A} N(\mathfrak{p})^{-s}=-C_A\log(s-1)+O(\log(s-1))$ ($s\to1^+$ 时). 这只需证明：对于每个 $\varepsilon>0$ 均有 $M=M(\varepsilon)$ 使得当 s 与1充分接近时均有

$$\Big|\sum_{\substack{\mathfrak{p}\in A\\ N(\mathfrak{p})\geqslant M}} N(\mathfrak{p})^{-s}+C_A\log(s-1)\Big|\leqslant\varepsilon|\log(s-1)| \tag{1}$$

即可. 为证此，我们取 M，使得 $x>M$ 时

$$|\pi(x, A)-C_Ax/\log x|<\varepsilon x/\log x,$$

则

$$\Big|\sum_{n=M}^{\infty}\pi(n, A)(n^{-s}-(n+1)^{-s})-\sum_{n=M}^{\infty}C_A\frac{n}{\log n}(n^{-s}-(n+1)^{-s})\Big|$$

$$\leqslant\varepsilon\sum_{n=M}^{\infty}\frac{n}{\log n}(n^{-s}-(n+1)^{-s}). \tag{2}$$

令 $$T(s)=\sum_{\substack{\mathfrak{p}\in A\\ N(\mathfrak{p})\geqslant M}} N(\mathfrak{p})^{-s}=\sum_{n=M}^{\infty}(\pi(n, A)-\pi(n-1, A))n^{-s},$$

$$U(s)=\sum_{n=M}^{\infty}\frac{n/\log n-(n-1)/\log(n-1)}{n^s}$$

$$=\sum_{n=M}^{\infty}\frac{1}{n^s\log n}+O(1),$$

由(2)式可知 $|T(s)-C_AU(s)|\leqslant\varepsilon U(s)$. 因此，为证(1)式，只需再证

$$\sum_{n=M}^{\infty}\frac{1}{n^s\log n}=-\log(s-1)+O(1)\quad(s\to1^+) \tag{3}$$

即可. 当 $1<s\leqslant2$, $s\leqslant t\leqslant2$ 时,

$$\int_s^2\Big(\sum_{n=M}^{\infty}n^{-t}\Big)\mathrm{d}t=\sum_{n=M}^{\infty}\Big(\frac{1}{n^s\log n}-\frac{1}{n^2\log n}\Big)$$

$$=\sum_{n=M}^{\infty}\frac{1}{n^s\log n}+O(1)$$

(交换$\int$和$\sum$是由于一致收敛性). 另一方面,

$$\int_s^2\left(\sum_{n=M}^{\infty}n^{-t}\right)\mathrm{d}t=\int_s^2\left(\zeta(t)-\sum_{n=1}^{M-1}n^{-t}\right)\mathrm{d}t$$
$$=\int_s^2\frac{\mathrm{d}t}{t-1}+O(1)=-\log(s-1)+O(1).$$

将以上两式放在一起即为(3)式,从而也就证明了引理. ▮

由此引理我们知道,全体素数所成集合的D-密度为1. 更一般地,对于每个数域K, K中全体素理想所成集合的D-密度是1.

2.2 素理想的分裂和多项式的分裂

现在我们给出计算$\delta(A)$的新的例子.

定理3 设L/K是数域的伽罗华扩张, $n=[L:K]$. 令$A=\{K$中素理想$\mathfrak{p}\mid\mathfrak{p}$在$L$中完全分裂$\}$, 则$\delta(A)=1/n$.

证明 当$s>1$时

$$\log\zeta_L(s)=\sum_{\mathfrak{P}}N_{L/\mathbb{Q}}(\mathfrak{P})^{-s}+O(1)$$
$$=\sum_{\mathfrak{p}}\sum_{\mathfrak{P}|\mathfrak{p}}N_{L/\mathbb{Q}}(\mathfrak{P})^{-s}+O(1)\qquad(1)$$

由于只有有限个$\mathfrak{p}$在L中分歧,它们不影响对$\delta(A)$的计算. 从而将它们排除之后,我们有$\mathfrak{p}=\mathfrak{P}_1\cdots\mathfrak{P}_g$, $gf=n$. 当$f\geqslant2$时, $N_{L/\mathbb{Q}}(\mathfrak{P})^{-s}=N_{K/\mathbb{Q}}(\mathfrak{p})^{-fs}\leqslant N_{K/\mathbb{Q}}(\mathfrak{p})^{-2s}$. (1)式右边对应于$f\geqslant2$的那些项在$s\geqslant1$时一致收敛. 而应$f=1$(即$\mathfrak{p}\in(A)$时, $\mathfrak{p}$有n个因子$\mathfrak{P}$, $N_{L/\mathbb{Q}}(\mathfrak{P})=N_{K/\mathbb{Q}}(\mathfrak{p})$. 因此

$$\log\zeta_L(s)=\sum_{\mathfrak{p}\in A}\sum_{\mathfrak{P}|\mathfrak{p}}N_{L/\mathbb{Q}}(\mathfrak{P})^{-s}+O(1)$$
$$=n\sum_{\mathfrak{p}\in A}N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}+O(1).$$

另一方面, $\log\zeta_L(s)=-\log(s-1)+O(1)\ (s\to1^+)$. 于是

$$\lim_{s\to1^+}\frac{\sum\limits_{\mathfrak{p}\in A}N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}{-\log(s-1)}=\lim_{s\to1^+}\frac{\frac{1}{n}\log\zeta_L(s)+O(1)}{\log\zeta_L(s)+O(1)}=\frac{1}{n},$$

即
$$\delta(A)=\frac{1}{n}.\qquad ▮$$

如果 L/K 不是伽罗华扩张，我们有

系 1 设 L/K 是数域的扩张，N 是 L 在 K 上的正规闭包，令 $A=\{K$ 中素理想 $\mathfrak{p}|\mathfrak{p}$ 在 L 中完全分裂$\}$. 则

$$\delta(A)=1/[N:K].$$

证明 令 $A'=\{K$ 中素理想 $\mathfrak{p}|\mathfrak{p}$ 在 N 中完全分裂$\}$. 由于 $K\subseteq L\subseteq N$，可知对每个 $\sigma\in G=\mathrm{Gal}(N/K)$ 均有 $K\subseteq\sigma(L)\subseteq N$. 现设 $\mathfrak{p}\in A$，令 $\mathfrak{P}$ 为 N 中素理想，$\mathfrak{P}|\mathfrak{p}$. 由于 $\mathfrak{p}$ 在 L 中完全分裂，从而关于 $\mathfrak{P}$ 的分解域 $K_D\supseteq L$(为什么？). 同样地，对于每个 $\sigma\in G$，$\mathfrak{p}$ 在 $\sigma(L)$ 中也是完全分裂的(为什么？). 因此 $K_D\supseteq\sigma(L)$. 于是 $N\supseteq K_D\supseteq\bigcup_{\sigma\in G}\sigma(L)=N$，从而 $K_D=N$. 这表明 $\mathfrak{p}$ 在 N 中完全分裂，即 $\mathfrak{p}\in A'$. 反之，若 $\mathfrak{p}\in A'$，即 $\mathfrak{p}$ 在 N 中完全分裂，从而在 L 中显然也完全分裂，因此 $\mathfrak{p}\in A$，这就表明 $A=A'$. 然后由定理 4 即知 $\delta(A)=\delta(A')=1/[N:K]$. ▮

定义 2 设 A 和 A' 是数域 K 中两个素理想集合. 定义

$$A\triangle A'=(A-A')\cup(A'-A)$$

(其中 $A-A'=\{\mathfrak{p}|\mathfrak{p}\in A,\ \mathfrak{p}\notin A'\}$).

如果 $\delta(A\triangle A')=0$，我们便称 A 和 A' 几乎相等，并且表示成 $A\overset{p.p.}{=\!=}A'$. 特别若 A 和 A' 只相差一个有限集合时(即 $|A\triangle A'|<+\infty$ 时)，则 $A\overset{p.p.}{=\!=}A'$.

系 2(Brauer) 设 L_1/K，L_2/K 均为数域的伽罗华扩张. 令 $S_i=\{K$ 中素理想 $\mathfrak{p}|\mathfrak{p}$ 在 L_i 中完全分裂$\}$，$i=1,2$. 如果 $S_1\overset{p.p.}{=\!=}S_2$，则 $L_1=L_2$.

证明 令 $L=L_1L_2$，$S=\{K$ 中素理想 $\mathfrak{p}|\mathfrak{p}$ 在 L 中完全分裂$\}$，则 L/K 也是伽罗华扩张. 并且我们在第二章中证明了：$\mathfrak{p}$ 在 L 中完全分裂 $\Leftrightarrow$ $\mathfrak{p}$ 在 L_1 和 L_2 中均完全分裂. 换句话说，$S=S_1\cap S_2$. 根据定理 4，$\delta(S)=1/[L:K]$，$\delta(S_i)=1/[L_i:K]$. 由于 $S_1\overset{p.p.}{=\!=}S_2$，从而 $S\overset{p.p.}{=\!=}S_i(i=1,2)$. 于是 $[L:K]=1/\delta(S)=1/\delta(S_i)=[L_i:K]$. 但是 $L_i\subseteq L$，因此 $L_i=L(i=1,2)$，于是

$L_1=L_2$. ∎

注记 定理 4 表明，如果 L/K 是数域的伽罗华扩张，则 K 中存在相当多(D–密度为 $1/[L:K]$)的素理想 $\mathfrak{p}$ 在 L 中完全分裂. 而系 2 表明，这些完全分裂的素理想组成的集合也完全决定了伽罗华扩域 L.

现在我们将定理 4 及其系用于有限域上多项式的因子分解问题. 设 L/K 是数域的扩张，$L=K(\theta)$，$\theta\in O_L$，$f(x)\in O_K[x]$是 θ 在 K 上的极小多项式，则 $f(x)$是不可约的首 1 多项式，并且 $\deg f(x)=n=[L:K]$. 我们在第二章中看到，除了有限多个可能之外，对于 K 中每个在 L 中不分歧的素理想 $\mathfrak{p}$，$\mathfrak{p}O_L$ 在 O_L 中的分解型式$\left(\text{即 } \mathfrak{p}O_L=\mathfrak{P}_1\cdots\mathfrak{P}_g \text{ 的参数 } g \text{ 和 } f_i=f(\mathfrak{P}_i|\mathfrak{p})\ (1\leqslant i\leqslant g),\ \sum_{i=1}^{g}f_i=n\right)$与多项式 $f(x)$在有限域 $O_K/\mathfrak{p}$ 上的分解型式是一样的. 于是由定理 4 中关于 $\mathfrak{p}$ 的完全分裂性结果可以推得 $f(x) \pmod{\mathfrak{p}}$ 的完全分裂结果. 为简单起见我们只考虑 $K=\mathbb{Q}$ 的情形. 虽然对于一般情形其结果也是对的.

定义 3 设 $f(x)\in\mathbb{Z}[x]$是 $\mathbb{Z}$ 上的首 1 不可约 n 次多项式，p 为素数. 如果 $f(x)$在 p 元域 $\mathbb{Z}/p\mathbb{Z}$ 上分解成 n 个不同的一次因子之积(这相当于说 $f(x)$在 $\mathbb{Z}/p\mathbb{Z}$ 中有 n 个不同的根)，则称 $f(x)$ **对于模 p 是完全分裂的**. 令 $S(f)=\{\text{素数 } p \mid f(x)\text{对模 } p \text{ 完全分裂}\}$.

令 $\theta\in\mathbb{C}$ 为 $f(x)$的一个根，$K=\mathbb{Q}(\theta)$. 如果 $K/\mathbb{Q}$ 是伽罗华、Abel 或者循环扩张，则 $f(x)$也分别叫作是**正规**, **Abel** 或者**循环多项式**.

根据上述素理想分解型式和多项式型式之间的关系，由定理 4 立即推出：

系 3 设 $f(x)$, $g(x)\in\mathbb{Z}[x]$ 均是首 1 不可约正规多项式，α, $\beta\in\mathbb{C}$ 分别是 $f(x)$和 $g(x)$的根. 如果 $S(f)\overset{\text{p.p.}}{=\!=}S(g)$，则

$$\deg f=\deg g,$$

并且 $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$。 ∎

注记 系 3 中关于 f 和 g 均为“正规”多项式这一假定是不可去掉的. Kronecker 最早研究这一问题. Gassmann 于 1926 年证明存在两个 180 次(!)的不可约多项式 f 和 g，除了有限多个素数之外对于每个素数 p，$f(x)$ 和 $g(x)$ 模 p 均有相同的分解型式. 但是对 $f(x)$ 的每个根 $\alpha\in\mathbb{C}$ 和 $g(x)$ 的每个根 $\beta\in\mathbb{C}$，均有 $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\beta)$. 1970 年 I. Gerst 给出更简单的例子：$f(x)=x^8-3\cdot 2^4$ 和 $g(x)=x^8-3^7$ 具有上述性质.

从系 1 立刻推得：

系 4 设 $f(x)\in\mathbb{Z}[x]$ 是首 1 不可约多项式，N 是 $f(x)$ 的分裂域，则 $\delta(S(f))=1/[N:\mathbb{Q}]$. ∎

同样地可以证得：

系 5 设 $f(x)$，$g(x)\in\mathbb{Z}[x]$ 均是首 1 不可约多项式. α，$\beta\in\mathbb{C}$ 分别为 $f(x)$ 和 $g(x)$ 的根. 如果 $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$，则

$$S(f)\xlongequal{\text{p.p.}}S(g).$$

证明 事实上，令 $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$. 我们已经知道，除了有限个之外的所有素数 p（即对所有 $p\nmid d(f)d(g)$ 的素数 p），p 在 K 中素理想分解的型式与 $f(x)$ 和 $g(x)$ 模 p 分解的型式均是相同的. 这就表明 $S(f)\triangle S(g)$ 是有限集合. 特别地有

$$S(f)\xlongequal{\text{p.p.}}S(g).\qquad ∎$$

例 可以证明 $f(x)=x^4+4x^3-4x^2-40x-56$ 和 $g(x)=x^4-8x^2-24x-20$ 均是 $\mathbb{Z}[x]$ 中不可约多项式，并且有相同的判别式：$d(f)=d(g)=-2^{12}\cdot 3^2\cdot 31$. 但是对于 $p=13\nmid d(f)d(g)$，$f(2)\equiv 0 \pmod{13}$，而 $g(x)$ 在 $\mathbb{Z}/13\mathbb{Z}$ 中无根. 于是由系 5 的证明即知对于 $f(x)$ 的任一根 $\alpha\in\mathbb{C}$ 和 $g(x)$ 的任一根 $\beta\in\mathbb{C}$，均有 $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\beta)$.

2.3 Abel L-函数，Чеботарёв 密度定理

设 L/K 为数域的伽罗华扩张. 我们在定理 4 中证明了，在

L 上完全分裂的 K 中素理想全体的 D 密度为 $1/[L:K]$. 现在我们要提出更一般的问题: 在 L 上分解型式为 (f, g) $(fg=[L:K])$ 的 K 中素理想全体的 D-密度是多少? (当 $g=[L:K]$, $f=1$ 时就是完全分裂的情形). 我们先解答 L/K 为 Abel 扩张的情形(定理 5 的系 1), 然后再解答 L/K 为伽罗华扩张的情形.

定理 4(Dirichlet 定理) 设 L/K 是数域的 Abel 扩张. 对于每个 $\sigma\in G=\mathrm{Gal}(L/K)$, 令 $A(\sigma)=\left\{K \text{ 中素理想 } \mathfrak{p} \mid \mathfrak{p} \text{ 在 } L \text{ 中不分歧, 并且} \left(\frac{L/K}{\mathfrak{p}}\right)=\sigma\right\}$, 则 $\delta(A(\sigma))=1/[L:K]$.

证明 定理 4 的证明是很不简单的. 这需要把解析数论的整个思想重演一遍, 而且我们不得不略去证明中最本质的部分(即下面的(C)). 首先, 我们需要构作新的 D-级数.

设 $\mathfrak{P}|\mathfrak{p}$, 其中 $\mathfrak{p}$ 和 $\mathfrak{P}$ 分别为 K 和 L 中素理想. 固定一个元素 $\sigma_{\mathfrak{p}}\in D_{\mathfrak{p}}$ ($D_{\mathfrak{P}}$ 是 $\mathfrak{p}$ 对于 L/K 的分解群), 并且使得 $\sigma_{\mathfrak{p}}$ 是扩张 $\bar{L}/\bar{K}$ $(\bar{L}=O_L/\mathfrak{P}, \bar{K}=O_K/\mathfrak{p})$ 之 Frobenius 自同构 $\bar{\sigma}$: $x\mapsto x^{|\bar{K}|}$ $(x\in\bar{L})$ 的一个原象. 于是 $\bar{\sigma}$ 的原象全体为 $\sigma_{\mathfrak{p}}I_{\mathfrak{p}}=\{\sigma_{\mathfrak{p}}\sigma \mid \sigma\in I_{\mathfrak{p}}\}$. 对于每个 $\chi\in\hat{G}$, (即 χ 为有限 Abel 群 $G=\mathrm{Gal}(L/K)$ 的特征), 定义

$$\chi(\mathfrak{p})=\chi(\sigma\mathfrak{p})\cdot\frac{1}{e(\mathfrak{P}|\mathfrak{p})}\sum_{\sigma\in I_{\mathfrak{p}}}\chi(\sigma).$$

不难看出:

(1) $\chi(\mathfrak{p})$ 与 $\sigma_{\mathfrak{p}}$ 之选取无关;

(2) 若 $I_{\mathfrak{p}}\nsubseteq\mathrm{Ker}\,\chi$, 则 χ 在 $I_{\mathfrak{p}}$ 上不是平凡特征. 从而由正交关系即知 $\chi(\mathfrak{p})=0$.

(3) 若 $I_{\mathfrak{p}}\subseteq\mathrm{Ker}\,\chi$, 则 $\chi(\mathfrak{p})=\chi(\sigma_{\mathfrak{p}})$ (因为 $|I_{\mathfrak{p}}|=e(\mathfrak{P}|\mathfrak{p})$).

(iv) 若 $\mathfrak{p}$ 在 L 中不分歧, 则 $I_{\mathfrak{p}}=\{1\}$, 从而

$$\chi(\mathfrak{p})=\chi\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right).$$

然后将 χ 的定义完全积性地扩充到 K 的全部非零整理想上. 也就是说, 若 $\mathfrak{a}=\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}$, 则 $\chi(\mathfrak{a})=\chi(\mathfrak{p}_1)^{a_1}\cdots\chi(\mathfrak{p}_r)^{a_r}$. 现在定义 D-级数

$$L(s,\ \chi,\ L/K)=\sum_{\mathfrak{a}}\chi(\mathfrak{a})N(\mathfrak{a})^{-s}\quad(\mathrm{Re}(s)>1),$$

其中 $\mathfrak{a}$ 过 K 的全部非零整理想. 于是:

(a) 由于 $|\chi(\mathfrak{a})|=0$ 或 1, 从而 $L(s,\ \chi,\ L/K)$ 在 $\mathrm{Re}(s)>1$ 中定义出正则函数,并且有 Euler 乘积公式

$$L(s,\ \chi,\ L/K)=\prod_{\mathfrak{p}}(1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}\quad(\mathrm{Re}(s)>1),$$

我们称 $L(s,\ \chi,\ L/K)$ 为 Abel 扩张 L/K 的 **Abel L-函数**.

(b) $\prod_{\chi\in\hat{G}}L(s,\ \chi,\ L/K)=\zeta_L(s)\quad(\mathrm{Re}(s)>1)$.

由于双方均有 Euler 乘积展开, 我们只需对 K 中每个素理想 $\mathfrak{p}$, 证明

$$\prod_{\chi\in\hat{G}}(1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s})=\prod_{\mathfrak{P}|\mathfrak{p}}(1-N(\mathfrak{P})^{-s})\tag{1}$$

即可. 由上面的(ii)和(iii)可知(1)式左边为

$$\prod_{\substack{\chi\in\hat{G}\\ \mathrm{Ker}\chi\supseteq I_{\mathfrak{p}}}}(1-\chi(\mathfrak{p})(N\mathfrak{p})^{-s})=\prod_{\chi\in(G/I_{\mathfrak{p}})^{\wedge}}(1-\chi(\sigma_{\mathfrak{p}})(N_{\mathfrak{p}})^{-s}).\tag{2}$$

令 $\mathfrak{p}O_L=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$, $efg=n$. 由于 $|G/I_{\mathfrak{p}}|=fg$, 而由 $\sigma_{\mathfrak{p}}$ 的取法知 $\sigma_{\mathfrak{p}}$ 在 $G/I_{\mathfrak{p}}$ 中的阶为 f. 从而 (2) 式右边为 $(1-N(\mathfrak{p})^{-fs})^g=\prod_{\mathfrak{P}|\mathfrak{p}}(1-(N(\mathfrak{P})^{-s})$. 这里我们用到下面的事实: 若 H 为 fg 阶 Abel 群, h 为 H 中 f 阶元素. 则 $\prod_{\chi\in\hat{H}}(1-\chi(h)x)=(1-x^f)^g$.

(c) $L(s,\ \chi,\ L/K)$ 可以解析延拓到整个复平面上. 当 $\chi\neq\chi_0$ 时, $L(s,\chi,L/K)$ 是整个复平面上的正则函数. 而 $L(s,\ \chi_0,\ L/K)$ 只在 $s=1$ 处有极点并且是单极点.

关于(c)的证明是很不平凡的. 这是因为, 如果我们考查 $L(s,\ \chi,\ L/K)=\sum_{\mathfrak{a}}\chi(\mathfrak{a})N(\mathfrak{a})^{-s}$ 的定义, 我们是从伽罗华群 $G=\mathrm{Gal}(L/K)$ 的特征定义出 K 的整理想集合上的一个函数. 要弄清 $L(s,\ \chi,\ L/K)$ 的解析性质, 就需要弄清 $\mathrm{Gal}(L/K)$ 和 K 的理想类群 $C(K)$ (或者更一般地,所谓 ray 理想类群)之间的关系. 而这正是类域论的一个最基本问题. 基于类域论的某些很不平凡的事实,我们可以证明(c).

有了这些准备,我们可以很容易证明定理 5,我们只需证明

$$\lim_{s\to1^+}\prod_{\mathfrak{p}\in A(\sigma)}N(\mathfrak{p})^{-s}/\log\zeta_K(s)=\frac{1}{n},\quad n=[L:K].$$

令 $T(s)=\dfrac{1}{n}\sum\limits_{\chi\in\hat{G}}\chi(\sigma^{-1})\log L(s,\ \chi,\ L/K)$，则由上面的(b)和(c)可知当 $\chi\neq\chi_0$ 时，$L(1,\ \chi,\ L/K)\neq0,\ \infty$，从而

$$\begin{aligned}&\lim_{s\to1^+}T(s)/\log\zeta_K(s)\\&=\frac{1}{n}+\lim_{s\to1^+}\sum_{\chi\neq\chi_0}\chi(\sigma^{-1})\log L(s,\ \chi,\ L/K)/\log\zeta_K(s)=\frac{1}{n}.\end{aligned}$$

另一方面，

$$\begin{aligned}T(s)&=\frac{1}{n}\sum_{\chi\in\hat{G}}\chi(\sigma^{-1})\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{1}{m}\chi(\mathfrak{p})^mN(\mathfrak{p})^{-ms}\\&=\frac{1}{n}\sum_{\chi\in\hat{G}}\chi(\sigma^{-1})\sum_{\mathfrak{p}}\chi(\mathfrak{p})N(\mathfrak{p})^{-s}+g(s)\\&=\frac{1}{n}\sum_{\mathfrak{p}}N(\mathfrak{p})^{-s}\sum_{\chi\in\hat{G}}\chi(\sigma^{-1})\chi(\mathfrak{p})+g(s)\\&\qquad(\mathrm{Re}(s)>1).\end{aligned}$$

这里 $g(s)$ 是对 $m\geqslant2$ 的求和部分．如同以前一样可知，$g(s)$ 在 $s=1$ 附近是有界的．但是除了有限个 $\mathfrak{p}$ 之外，$\chi(\mathfrak{p})=\chi\left(\left(\dfrac{L/K}{\mathfrak{p}}\right)\right)$．而

$$\sum_{\chi\in\hat{G}}\chi(\sigma^{-1})\chi\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right)=\begin{cases}n, & 若\left(\dfrac{L/K}{\mathfrak{p}}\right)=\sigma;\\0, & 否则.\end{cases}$$

因此
$$\frac{1}{n}=\lim_{s\to1^+}\frac{T(s)}{\log\zeta_K(s)}=\lim_{s\to1^+}\frac{\sum\limits_{\mathfrak{p}\in A(\sigma)}N(\mathfrak{p})^{-s}}{\log\zeta_K(s)}$$

这就证明了定理 4． ▮

系 1 设 L/K 是 Abel 扩张，$fg=n=[L:K]$．以 n_f 表示 $G=\mathrm{Gal}(L/K)$ 中 f 阶元素的个数，$A=\{K$ 中素理想 $\mathfrak{p}\mid\mathfrak{p}$ 在 L 中素理想分解的型式为 $(f,\ g)\}$．则 $\delta(A)=n_f/n$．

证明 如果 $\mathfrak{p}$ 在 L 中不分歧并且 $\mathfrak{p}\in A$，则 $\left(\dfrac{L/K}{\mathfrak{p}}\right)$ 为 G 中 f 阶元素．设 G 中 n_f 个 f 阶元素为 $\sigma_1,\ \cdots,\ \sigma_{n_f}$．由定理 5 知

$$\delta(A(\sigma_i))=\frac{1}{n}\quad(1\leqslant i\leqslant n_f).$$

而 A 是 n_f 个两两非交集合 $A(\sigma_i)$ 的并集．从而 $\delta(A)=n_f/n$． ∎

例 设 L/K 是数域的 Abel 扩张，并且 $G=\mathrm{Gal}(L/K)$ 是两个 2 阶循环群的直积．则 G 中有一个 1 阶元素和三个 2 阶元素．从而在 L 中完全分裂的 K 中素理想集合的 D-密度为 1/4．而 $\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2(\mathfrak{P}_1\neq\mathfrak{P}_2)$ 的 K 中素理想集合的 D-密度为 3/4．最后，在 L 中惯性的 K 中素理想集合的 D-密度为 0，因为 G 中没有 4 阶元素．

我们将定理 4 叫作是 Dirichlet 定理，是因为通常关于算术级数的 Dirichlet 定理(的弱形式)是定理 5 的特例．

系 2 设 $(l,\ k)=1,\ k\geqslant1$．$A=\{$素数 $p\mid p\equiv l(\mathrm{mod}\,k)\}$，则 $\delta(A)=1/\varphi(k)$．

证明 取 $K=\mathbb{Q}$，$L=\mathbb{Q}(\zeta_k)$．则 $[L:\mathbb{Q}]=\varphi(k)$．

$$G=\mathrm{Gal}(L/\mathbb{Q})=\{\sigma_l\mid(l,\ k)=1\},$$

其中 $\sigma_l(\zeta_k)=\zeta_k^l$．若 p 在 L 中不分歧(即 $p\nmid k$)，我们已经证明过 $\left(\frac{L/K}{p}\right)=\sigma_p$，因此 $\left(\frac{L/K}{p}\right)=\sigma_l\Leftrightarrow p\equiv l(\mathrm{mod}\,k)$．于是由定理 5 即知 $\delta(A)=\delta\left(\left\{p\,\middle|\left(\frac{L/K}{p}\right)=\sigma_l\right\}\right)=1/\varphi(k)$． ∎

注记

1．从定理 5 证明中的(c)可知

$$\zeta_L(s)/\zeta_K(s)=\prod_{\substack{\chi\neq\chi_0\\ \chi\in\hat{G}}}L(s,\ \chi,\ L/K)$$

是整个复平面上的正则函数．换句话说，(利用类域论)可以证明当 L/K 为数域的 Abel 扩张时，Artin 猜想是成立的．

2．我们从定理 5 推导出了系 2 (关于算术级数中素数的 Dirichlet 定理的弱形式)．反过来，利用系 2 和 Abel 域中的互反律(第二章定理 20) 的证明也可以(不用类域论)推出：对于 $L/\mathbb{Q}$ 为 Abel 扩张的情形(即对于定理 5 中 $K=\mathbb{Q}$ 的情形) 定理 5 是对的．(习题 11)．这就给出定理 5 对于 $K=\mathbb{Q}$ 情形的一个完全的

证明.

现在讨论 L/K 为伽罗华扩张的情形. 这时,设 K 中素理想 $\mathfrak{p}$ 在 L 中不分歧, 则 $\mathfrak{p}O_L=\mathfrak{P}_1\cdots\mathfrak{P}_g$, 令 $\mathfrak{P}=\mathfrak{P}_1$. 则每个 $\mathfrak{P}_i$ 均可写成 $\sigma(\mathfrak{P})$, (对某个 $\sigma\in G=\mathrm{Gal}(L/K)$). 但是

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)=\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1},$$

于是 $\left\{\left(\frac{L/K}{\mathfrak{P}_i}\right)\middle|1\leqslant i\leqslant g\right\}=\left\{\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}\middle|\sigma\in G\right\}$, 这是有限群 G 的一个共轭类, 我们将这个共轭类表示成 $\left(\frac{L/K}{\mathfrak{p}}\right)$. $\Big($当 L/K 为 Abel 扩张时, 这个共轭类只含有一个元素, 我们曾经把这个元素表示成 $\left(\frac{L/K}{\mathfrak{p}}\right)\Big)$.

定理 5(Чеботарёв) 设 L/K 是数域的伽罗华扩张, $G=\mathrm{Gal}(L/K)$. C 为 G 中一个共轭元素类 $|C|=c$. $A=\left\{K\text{ 中素理想 }\mathfrak{p}\middle|\mathfrak{p}\text{ 在 }L\text{ 中不分歧并且}\left(\frac{L/K}{\mathfrak{p}}\right)=C\right\}$, 则 $\delta(A)=c/n$, $n=[L:K]$.

证明 俄国数学家 Чеботарёв 原来的证明很复杂. 这里采用 1969 年 McCluer 给出的简化证明. 首先需要下列的引理.

引理 5 设 L/K 是数域的伽罗华扩张, $\mathfrak{P}$ 和 $\mathfrak{p}$ 分别是 L 和 K 中的(固定)素理想, $\mathfrak{P}|\mathfrak{p}$. $\mathfrak{p}$ 在 L 中不分歧. M 是 L/K 的中间域. 并且对于 M 中每个素理想 $\mathfrak{q}|\mathfrak{p}$, $\mathfrak{q}$ 在 L 中均是惯性的(从而 $\mathfrak{q}O_L$ 为 L 中素理想). 令 $\left(\frac{L/K}{\mathfrak{P}}\right)=\sigma\in G=\mathrm{Gal}(L/K)$. 则 $\mathfrak{p}$ 在 M 中共存在 $[C_G(\sigma):H]$ 个素理想因子 $\mathfrak{q}$, 使得 $\left(\frac{L/K}{\mathfrak{q}O_L}\right)=\sigma$. 其中 $C_G(\sigma)=\{\tau\in G|\tau\sigma=\sigma\tau\}$ (σ 在 G 中的中心化子), 而 $H=\langle\sigma\rangle$ (σ 在 G 中生成的循环子群).

这是因为: 从引理的假设可知, 我们只需证明 L 中共有 $[C_G(\sigma):H]$ 个 $\mathfrak{P}'|\mathfrak{p}$ 使得 $\left(\frac{L/K}{\mathfrak{P}'}\right)=\sigma$. 每个这种 $\mathfrak{P}'$ 均可写成

$\tau(\mathfrak{P})$, $\tau\in G$. 而

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right)=\sigma\Leftrightarrow\tau\sigma\tau^{-1}=\sigma\Leftrightarrow\tau\in C_G(\sigma);$$

并且 $\tau_1\mathfrak{P}=\tau_2\mathfrak{P}\Leftrightarrow\tau_2^{-1}\tau_1\mathfrak{P}=\mathfrak{P}\Leftrightarrow\tau_2^{-1}\tau_1\in D_{\mathfrak{P}}=\langle\sigma\rangle=H$.

由此即得引理.

现在证明定理 5. 这只需证明

$$\sum_{\left(\frac{L/K}{\mathfrak{p}}\right)=C} N(\mathfrak{p})^{-s}=-\frac{c}{n}\log(s-1)+o(\log(s-1))$$

(当 $s\to1^+$ 时).

取 $\sigma\in C$, $H=\langle\sigma\rangle\subseteq G=\mathrm{Gal}(L/K)$. M 为 H 的固定子域, 则 $\mathrm{Gal}(L/M)\cong H$, 从而 L/M 为循环扩张. 由定理 5 知

$$\sum_{\left(\frac{L/M}{\mathfrak{q}}\right)=\sigma} N(\mathfrak{q})^{-s}=-\frac{1}{|H|}\log(s-1)+o(\log(s-1)).$$

从而 $$\sum_{\substack{\mathfrak{q},\mathfrak{p}\\ \left(\frac{L/M}{\mathfrak{q}}\right)=\sigma\\ f(\mathfrak{q},\mathfrak{p})=1}} N(\mathfrak{p})^{-s}=-\frac{1}{|H|}\log(s-1)+o(\log(s-1)).$$

对于使$\left(\frac{L/M}{\mathfrak{q}}\right)=\sigma$ 和 $\mathfrak{q}|\mathfrak{p}$ 成立的每个 $\mathfrak{p}$, M 满足上面引理条件. 因为$\left(\frac{L/M}{\mathfrak{q}}\right)=\sigma$, 则分解群 $D_{\mathfrak{p}}=\langle\sigma\rangle=H\cong\mathrm{Gal}(L/M)$, 从而 $\mathfrak{q}$ 在 L 中惯性. 若 $\mathfrak{q}'$ 为 M 中素理想并且 $\mathfrak{q}'|\mathfrak{p}$, 则 $D_{\mathfrak{q}'}$ 与 $D_{\mathfrak{q}}$ 共轭, 从而仍有 $|D_{\mathfrak{q}'}|=|\mathrm{Gal}(L/M)|$, 即 $\mathfrak{q}'$ 在 L 中惯性. 于是由引理得出$\left(注意\left(\frac{L/M}{\mathfrak{q}}\right)=\sigma\Leftrightarrow\left(\frac{L/K}{\mathfrak{p}}\right)=C\right)$.

$$[C_G(\sigma):H]\sum_{\left(\frac{L/K}{\mathfrak{p}}\right)=C} N(\mathfrak{p})^{-s}=-\frac{1}{|H|}\log(s-1)+o(\log(s-1)).$$

于是

$$\sum_{\left(\frac{L/K}{\mathfrak{p}}\right)=C} N(\mathfrak{p})^{-s}=-\frac{1}{[C_G(\sigma):H]\cdot|H|}\log(s-1)+o(\log(s-1)).$$

但是 $\frac{1}{[C_G(\sigma):H]\cdot|H|}=\frac{1}{|C_G(\sigma)|}=\frac{c}{n}$. 从而定理 5 证毕. ▌

由定理 5 立刻推出

系 定理 4 的系 1 对于数域的伽罗华扩张 L/K 也是对的.

证明 只需注意, $\mathrm{Gal}(L/K)$ 中彼此共轭的元素有相同的阶数. ▌

习 题

1. 设 $f(x)$ 和 $g(x)$ 为 $\mathbb{Z}[x]$ 中不可约多项式, α 和 $\beta\in\mathbb{C}$ 分别是 $f(x)$ 和 $g(x)$ 的根, $\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\beta)$, 则 $S(f)\overset{\text{p.p.}}{\supseteq}S(g)$. (即 $\delta(S(g)-S(f))=0$.)
2. 对于 $\mathbb{Z}[x]$ 中每个次数 $\geqslant 1$ 的不可约多项式 $f(x)$, $S(f)$ 均是无限集合.
3. 设 l 为素数. 求证对于每个次数 $\geqslant 1$ 的多项式 $f(x)\in\mathbb{Z}[x]$, 均有无限多个素数 $p\equiv 1(\mathrm{mod}\ l)$, 使得 $f(x)$ 模 p 完全分裂.
4. 设 $f_1(x), \cdots, f_r(x)$ 是 $\mathbb{Z}[x]$ 中有限个多项式, 并且 $\deg f_i\geqslant 1(1\leqslant i\leqslant r)$, 则存在无限多个素数 p, 使得 $f_1(x), f_2(x), \cdots, f_r(x)$ 均完全分裂.
5. 对于每个奇素数 p, 求证集合 $\left\{\text{素数 } q \,\middle|\, \left(\frac{q}{p}\right)=1\right\}$ 的 D-密度为 1/2.
6. 设 L/K 为循环扩张. 求证 K 中有无限多个素理想 $\mathfrak{p}$ 在 L 中惯性, 试问这种素理想 $\mathfrak{p}$ 所成的集合的 D-密度是多少?
7. (a) 设 p 为素数并且 $p\equiv 1(\mathrm{mod}\ 3)$. 求证 x^3-2 模 p 可约 $\Leftrightarrow x^3-2$ 模 p 完全分裂.

   (b) 计算素数集合 $\{p\,|\,2$ 为模 p 的三次剩余$\}$ 的 D-密度.
8. 计算素数集合 $\{p\,|\,2$ 为模 p 的四次剩余$\}$ 的 D-密度.
9. 设 $f(x)$ 是 $\mathbb{Z}[x]$ 中不可约首 1 多项式, $\deg f\geqslant 2$. $\alpha\in\mathbb{C}$ 为 $f(x)$ 的一个根, M 是 $f(x)$ 的分裂域, $L=\mathbb{Q}(\alpha)$.

   (a) 求证下面三个素数集合几乎(p. p.)相等:

   $\{p\,|\,f(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中有根$\}$;

   $\{p\,|\,L$ 中有素理想 $\mathfrak{p}|p$, 并且 $f(\mathfrak{p}|p)=1\}$;

   $\left\{p\,\middle|\,M \text{ 中有素理想}\mathfrak{P}|p, \text{并且}\left(\frac{M/\mathbb{Q}}{\mathfrak{P}}\right)a=a(\forall a\in L)\right\}$.

(b) 求证有无限多个素数 p 使得 $f(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中无根.

10. 对于 $\mathbb{Z}[x]$ 中每个不可约多项式 $f(x)$，求证均存在无限多素数 p，使得 $f(x)$ 在 $\mathbb{Z}/p\mathbb{Z}[x]$ 中仍不可约.

11. 用定理 5 的系 2 和 Abel 域互反律(第二章定理 20)的证明来推出本章定理 5 对于 $K=\mathbb{Q}$ 的情形(即 $L/\mathbb{Q}$ 为 Abel 扩张)是成立的.

第六章 Abel 数域的类数公式

§1 Hasse 类数公式

我们现在展示解析理论在研究代数数域类数问题中的应用。解析理论与类数问题的联系已经在第四章中给出，那就是：

$$\lim_{s\to1}(s-1)\zeta_K(s)=\frac{2^{r_1}(2\pi)^{r_2}R_Kh_K}{w_K|d(K)|^{1/2}}.$$

此式右边出现的数域 K 中的诸量 r_1, r_2, w_K, $|d(K)|^{1/2}$ 通常容易求得. R_K 与基本单位组有关，是难求的量. 对于此式的左边，我们则希望 $\zeta_K(s)$ 有更好的表达式. 高斯对于二次域作了这件事，从而得到了二次域类数相当简单的公式. 后来，在研究费尔马问题的推动之下，Kummer 对于分圆域也给出了类数解析公式. 到了本世纪三十年代之后，Hasse 对于一般的 Abel 数域给出类数解析公式，并且由此相当精细地研究了 Abel 域类数的各种问题. 其研究成果集中总结在他于 1952 年所写的“关于 Abel 域的类数”一书中.

对于 Abel 数域 K，$\zeta_K(s)$ 应当有好的表达式，这一点是不应当感到很奇怪的. 因为根据 Kronecker–Weber 定理，每个 Abel 数域均是分圆域的子域，而分圆域中有很简单的素理想分解规则. 设 $\mathbb{Q}(\zeta_m)$, $m\not\equiv2 \pmod 4$ 是包含 Abel 数域 K 的最小分圆域，即 $m=\mathrm{cond}(K)$（域 K 的导子）. 我们有如下的伽罗华对应：

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_m) & & \{1\} \\
| & & | \\
K & & H \\
| & & | \\
\mathbb{Q} & & G=\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})
\end{array}$$

由于

$$G\cong(\mathbb{Z}/m\mathbb{Z})^*,\ \sigma_a\mapsto a(\operatorname{mod} m),\ (a,\ m)=1,\ \sigma_a(\zeta_m)=\zeta_m^a.$$

从而 H 同构于 $(\mathbb{Z}/m\mathbb{Z})^*$ 的一个子群(我们今后常常把 H 和这个子群等同起来), 而 $\mathrm{Gal}(K/\mathbb{Q})$ 同构于商群 $(\mathbb{Z}/m\mathbb{Z})^*/H$ (我们也常把这两者等同起来). 有限 Abel 群 $\mathrm{Gal}(K/\mathbb{Q})=(\mathbb{Z}/m\mathbb{Z})^*/H$ 的每个特征 χ 也叫作是域 K 的特征, 而 $(\mathbb{Z}/m\mathbb{Z})^*/H$ 的特征群也叫作是 K 的特征群, 表示成 $\hat{K}$. 于是, $\hat{K}$ 实际上是由全部在 H 上平凡的模 m 的 D-特征所构成的.

设 χ 为模 m 的 D-特征, 则 χ 是由唯一决定的一个模 m' 的本原 D-特征所诱导出来的, 其中 $m'=\mathrm{cond}(\chi)$, $m'|m$. 我们将诱导出 χ 的这个本原 D-特征表示成 χ^*.

定理 1 (Hasse) 设 K 是 Abel 数域, 则

$$\zeta_K(s)=\prod_{\chi\in\hat{K}}L(s,\ \chi^*)=\zeta(s)\prod_{\substack{\chi\in\hat{K}\\ \chi\neq\chi_0}}L(s,\ \chi^*).$$

即 Dedekind zeta 函数 $\zeta_K(s)$ 是一些对本原 D-特征的 Dirichlet L-函数之乘积.

证明 根据解析延拓原理, 我们只要对 $\mathrm{Re}(s)>1$ 的情形证明上式即可. 而在 $\mathrm{Re}(s)>1$ 时, 双方均有 Euler 乘积公式: $\zeta_K(s)=\prod\limits_{p}\prod\limits_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s})^{-1}$, $L(s,\ \chi^*)=\prod\limits_{p}(1-\chi^*(p)p^{-s})^{-1}$. 从而只需对每个有理素数 p 证明

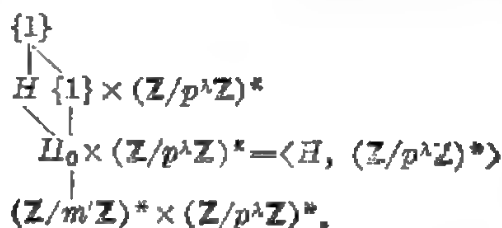
$$\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s})=\prod_{\chi\in\hat{K}}(1-\chi^*(p)p^{-s})\tag{1}$$

即可. 设

$$pO_K=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^e,\quad efg=n=[K:\mathbb{Q}],\quad N(\mathfrak{p}_i)=p^f,$$

则(1)式左边为 $(1-p^{-fs})^g$. 为了计算(1)式右边, 我们考虑如下的伽罗华对应图表: 令 $m=p^\lambda m'$, $(p,\ m')=1$, $\lambda\geqslant0$, $C_m=\mathbb{Q}(\zeta_m)$,





其中 H_0 为自然同态 λ: $\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m'\mathbb{Z}$, $a(\mathrm{mod}\ m)\mapsto a(\mathrm{mod}\ m')$ 之下的象 $\lambda(H)$. 我们前面说过, 每个特征 $\chi\in\hat{K}$ 均可看成是 $\mathrm{Gal}(K/\mathbb{Q})=(\mathbb{Z}/m\mathbb{Z})^*/H$ 的特征, 即是在 H 上平凡的模 m 的 D-特征. 如果 $p|\mathrm{cond}(\chi)$, 则 $\chi^*(p)=0$. 此时它对 (1) 式右边的贡献为 1. 而当 $\chi^*(p)\neq 0$ 时, 必然 $p\nmid\mathrm{cond}(\chi)|m=p^\lambda m'$, 于是 $\mathrm{cond}(\chi)|m'$, 即 χ^* 可看成是 $(\mathbb{Z}/m\mathbb{Z})^*/H$ 在 λ 之下的象 $(\mathbb{Z}/m'\mathbb{Z})^*/H_0$ 的特征. 从而

$$\prod_{\chi\in\hat{K}}(1-\chi^*(p)p^{-s})=\prod_{\chi\in((\mathbb{Z}/m'\mathbb{Z})^*/H_0)^\wedge}(1-\chi(p)p^{-s}).\qquad(2)$$

令 T 为 p 在 K 中的惯性域(极大不分歧子域), 则 $T=K\cap C_{m'}$(这是由于: p 在 $C_{m'}$ 中不分歧, 从而在 $K\cap C_{m'}$ 中也不分歧. 于是 $T\supseteq K\cap C_{m'}$. 另一方面, p 在 C_{p^λ} 中完全分歧, 从而 p 在 $T\cap C_{p^\lambda}$ 中也完全分歧. 所以 $T\cap C_{p^\lambda}=\mathbb{Q}$. 于是 T 的固定子群 $\supseteq$ $(\mathbb{Z}/p^\lambda\mathbb{Z})^*=C_{m'}$ 的固定子群. 从而 $T\subseteq C_{m'}$, 即 $T\subseteq C_{m'}\cap K$). 这就得出 $\mathrm{Gal}(T/\mathbb{Q})=\mathrm{Gal}(K\cap C_{m'}/\mathbb{Q})=(\mathbb{Z}/m'\mathbb{Z})^*/H_0$. 从而由(2)式即知

$$\prod_{\chi\in\hat{K}}(1-\chi^*(p)p^{-s})=\prod_{\chi\in\mathrm{Gal}(T/\mathbb{Q})}(1-\chi(p)p^{-s}).\qquad(3)$$

但是$[T:\mathbb{Q}]=fg$, 而 Frobenius 自同构$\left(\dfrac{C_{m'}/\mathbb{Q}}{p}\right)$相当于 $(\mathbb{Z}/m'\mathbb{Z})^*$ 中元素 $p(\mathrm{mod}\ m')$. 又由于$\left(\dfrac{C_{m'}/\mathbb{Q}}{p}\right)\Big|_T=\left(\dfrac{T/\mathbb{Q}}{p}\right)$, 而$\left(\dfrac{T/\mathbb{Q}}{p}\right)$(即元素 $p(\mathrm{mod}\ m')$)在 $\mathrm{Gal}(T/\mathbb{Q})$ 中的阶为 f. 从而由第四章 § 10, 习题 26 即知(3)式右边为 $(1-p^{-fs})^g$. 这就证明了(1)式, 从而也证明了定理 1. ▌

由定理 1 直接推出

系 设 K 为 Abel 数域, 则

$$\rho_K h_K=\prod_{\substack{\chi\in\hat{K}\\ \chi\neq\chi_0}}L(1,\ \chi^*),$$

其中
$$\rho_K=\frac{2^{r_1}(2\pi)^{r_2}R_K}{W_K|d(K)|^{1/2}}.$$ ▌

现在的问题是将 $L(1,\ \chi^*)$ 表示成尽可能明显、初等和便于计算的

形式。对于 χ 为奇特征（即 $\chi(-1)=-1$）和偶特征（即 $\chi(-1)=1$）两种情形，$L(1, \chi^*)$ 的表达式是不太相同的。

引理 1

(a) Abel 数域 K 为实域 $\Leftrightarrow$ K 的特征均为偶特征。

(b) 若 K 为虚 Abel 数域，K_+ 为 K 的极大实子域，则 $[K:K_+]=2$，并且 $\hat{K}_+$ 即为 $\hat{K}$ 中全部偶特征所形成的子群。

证明

(a) 假设 $\mathrm{Cond}(K)=m$，则有伽罗华对应

$$
\begin{array}{ccc}
C_m & \qquad & \{1\} \\
| & & | \\
K & & G \\
| & & | \\
\mathbb{Q} & & (\mathbb{Z}/m\mathbb{Z})^*
\end{array}
$$

于是 $\mathrm{Gal}(K/\mathbb{Q})=(\mathbb{Z}/m\mathbb{Z})^*/G$，而 $(\mathbb{Z}/m\mathbb{Z})^*$ 中的 $-1 \pmod m$ 相当于复共轭自同构 $\sigma_{-1}(\zeta_m)=\zeta_m^{-1}=\bar{\zeta}_m$。从而

K 为实域 $\Leftrightarrow$ σ_{-1} 为 K 中恒等自同构 $\Leftrightarrow$ $-1\in G$ $\Leftrightarrow$ -1 为 $(\mathbb{Z}/m\mathbb{Z})^*/G$ 中的单位元素 $\Leftrightarrow$ K 的每个特征（即 $(\mathbb{Z}/m\mathbb{Z})^*/G$ 的每个特征）均为偶特征。

(b) 若 K 为虚 Abel 数域，则 K 中有奇特征，于是 $\hat{K}$ 中偶特征全体形成 $\hat{K}$ 的指数为 2 的子群。此子群即是 $(\mathbb{Z}/m\mathbb{Z})^*/\langle -1, G\rangle$ 的特征群，而 $\langle -1, G\rangle$ 的固定子域就是 K 的极大实子域 K_+，由此即得 (b) 中结论。 ∎

由引理 1 我们有

$$\zeta_{K_+}(s)=\prod_{\chi\in\hat{K}_+} L(s,\chi^*)=\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=1}} L(s,\chi^*)=\zeta(s)\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=1\\ \chi\neq\chi_0}} L(s,\chi^*).$$

从而由定理 1 的系立刻得到

引理 2 (a) 设 K 为 n 次实 Abel 域，则

$$R_K h_K\cdot\frac{2^{n-1}}{|d(K)|^{1/2}}=\prod_{\substack{\chi\in\hat{K}\\ \chi\neq\chi_0}} L(1,\chi^*).$$

(b) 设 K 为 n 次虚 Abel 域，则

$$R_K h_K \cdot \frac{(2\pi)^{n/2}}{w_K |d(K)|^{1/2}} = \prod_{\substack{\chi\in\hat{R}\\ \chi\neq\chi_0}} L(1, \chi^*).$$

$$R_{K_+} h_{K_+} \cdot \frac{2^{n/2-1}}{|d(K_+)|^{1/2}} = \prod_{\substack{\chi_0\neq\chi\in\hat{R}\\ \chi(-1)=1}} L(1, \chi^*). \quad ∎$$

现在我们来计算 $L(1, \chi^*)$ 的值.

引理 3 设 χ 为模 m 本原 D-特征, $m\geqslant 3$, 则

$$L(1, \chi)=\begin{cases} -\dfrac{2G(1, \chi)}{m}\displaystyle\sum_{1\leqslant k<m/2}\overline{\chi}(k)\log\sin\frac{k\pi}{m}, \\ \qquad\qquad \text{当 } \chi(-1)=1 \text{ 时}; \\ \dfrac{\pi i G(1, \chi)}{m^2}\displaystyle\sum_{k=1}^{m-1}\overline{\chi}(k)k=\frac{\pi i G(1, \chi)}{m(\chi(2)-2)}\sum_{1\leqslant k<m/2}\overline{\chi}(k), \\ \qquad\qquad \text{当 } \chi(-1)=-1 \text{ 时}. \end{cases}$$

其中 $G(k, \chi)=\sum_{a=1}^{m-1}\chi(a)\zeta_m^{ak}$ 为 Gauss 和.

证明 记 $\omega=\zeta_m$, 当 $\mathrm{Re}(s)>1$ 时

$$\begin{aligned} L(s, \chi) &= \sum_{a=0}^{m-1}\chi(a)\sum_{\substack{n=1\\ n\equiv a(\bmod m)}}^{\infty} n^{-s} \\ &= \sum_{a=0}^{m-1}\chi(a)\sum_{n=1}^{\infty}\left(\frac{1}{m}\sum_{k=0}^{m-1}\omega^{(a-n)k}\right)n^{-s} \\ &= \frac{1}{m}\sum_{k=0}^{m-1}G(k, \chi)\sum_{n=1}^{\infty}\omega^{-nk}n^{-s} \\ &= \frac{G(1, \chi)}{m}\sum_{k=0}^{m-1}\overline{\chi}(k)\sum_{n=1}^{\infty}\omega^{-nk}n^{-s}. \end{aligned}$$

(交换和号是由于级数的绝对收敛性). 但是 D-级数 $\sum_{n=1}^{\infty}\omega^{-nk}n^{-s}$ 在 $\mathrm{Re}(s)>0$ 中正则, 从而它在 $s=1$ 处连续. 熟知它在 $s=1$ 处的值为 $-\log(1-\omega^{-k})$. 因此

$$\begin{aligned} L(1, \chi) &= -\frac{G(1, \chi)}{m}\sum_{k=0}^{m-1}\overline{\chi}(k)\log(1-\omega^{-k}) \\ &= -\frac{\chi(-1)G(1, \chi)}{m}\sum_{k=0}^{m-1}\overline{\chi}(k)\log(1-\omega^{k}). \end{aligned}$$

当 $0<k<m$ 时,

$$\log(1-\omega^k)=\log 2+\log\sin\frac{k\pi}{m}+\left(\frac{k}{m}-\frac{1}{2}\right)\pi i,$$

于是(由于 $\mathrm{Cond}(\chi)=m\geqslant 3$ 从而 $\chi\neq\chi_0$)

$$L(1,\chi)=-\frac{\chi(-1)G(1,\chi)}{m}\sum_{k=1}^{m-1}\bar{\chi}(k)\left(\log\sin\frac{k\pi}{m}+\frac{k\pi i}{m}\right).$$

当 $\chi(-1)=1$ 时 $\sum\bar{\chi}(k)k=0$ 而当 $\chi(-1)=-1$ 时

$$\sum\bar{\chi}(k)\log\sin\frac{k\pi}{m}=0$$

(习题),从而

$$L(1,\chi)=\begin{cases}-\dfrac{2G(1,\chi)}{m}\displaystyle\sum_{1<k<m/2}\bar{\chi}(k)\log\sin\frac{k\pi}{m}, \\ \qquad\qquad \chi(-1)=1\text{ 时};\\ \dfrac{\pi i G(1,\chi)}{m^2}\displaystyle\sum_{k=1}^{m-1}\bar{\chi}(k)k, \quad \chi(-1)=-1\text{ 时}.\end{cases}$$

最后再由下面引理 4,即得到引理 3 的全部结果. ▌

引理 4 设 χ 为模 m 的本原奇特征,则

$$\sum_{k=1}^{m-1}\chi(k)k=\frac{m}{\chi(2)-2}\sum_{1<k<m/2}\chi(k).$$

证明 如果$2\nmid m$,则

$$\begin{aligned}-\sum_{0<k<m}\chi(k)k&=-\sum_{\substack{k=0\\2|k}}^{m}(\chi(k)k+\chi(m-k)(m-k))\\&=-\sum_{0<k<m/2}\chi(2k)2k+\sum_{0<k<m/2}\chi(2k)(m-2k)\\&=\chi(2)\sum_{0<k<m/2}(m-4k)\chi(k).\end{aligned}$$

因此

$$-\bar{\chi}(2)\sum_{0<k<m}\chi(k)k=\sum_{0<k<m/2}(m-4k)\chi(k) \tag{1}$$

另一方面,

$$\begin{aligned}-\sum_{0<k<m}\chi(k)k&=-\sum_{0<k<m/2}\chi(k)k-\sum_{0<k<m/2}\chi(m-k)(m-k)\\&=-\sum_{0<k<m/2}\chi(k)k+\sum_{0<k<m/2}\chi(k)(m-k)\\&=\sum_{0<k<m/2}(m-2k)\chi(k).\end{aligned}$$

将此式与(1)式合在一起,即为

$$\sum_{0<k<m}\chi(k)k=\frac{m}{\overline{\chi}(2)-2}\sum_{0<k<m/2}\chi(k).$$

如果 $4|m$，则 $\chi(2)=0$，并且 $\chi(k+m/2)=-\chi(k)\ (0<k<m/2)$（这是因为：由 $(m/2+1)^2\equiv\frac{m}{4}\cdot m+m+1\equiv1\pmod m$ 可知 $\chi\left(\frac{m}{2}+1\right)=\pm1$。如果 $\chi\left(\frac{m}{2}+1\right)=1$，则由于对每个奇数 k 均有 $\left(\frac{m}{2}+1\right)k\equiv m/2+k\pmod m$，从而 $\chi(m/2+k)=\chi(k)$。于是导出矛盾 $m=\mathrm{cond}(\chi)|m/2$。因此 $\chi(m/2+1)=-1$，从而对于每个奇数 k 均有 $\chi(k+m/2)=-\chi(k)$。而对偶数 k 此式当然也是对的，因两边均为 0。于是

$$\begin{aligned}\sum_{0<k<m}\chi(k)k&=\sum_{0<k<m/2}\chi(k)k+\sum_{0<k<m/2}\chi(k+m/2)(k+m/2)\\&=\sum_{0<k<m/2}\chi(k)k-\sum_{0<k<m/2}\chi(k)(k+m/2)\\&=-\frac{m}{2}\sum_{0<k<m/2}\chi(k).\end{aligned}$$

即引理 4 对 $4|m$ 情形也成立。∎

将引理 3 代入引理 2 就得到

引理 5 以 f_χ 表示 D-特征 χ 的导子．则

(a) 对于 n 次实 Abel 数域 K，

$$R_Kh_K=|d(K)|^{1/2}\prod_{\chi_0\neq\chi\in\hat{K}}\frac{1}{\sqrt{f_\chi}}\left|\sum_{1\leq k<f_\chi/2}\chi(k)\log\sin\frac{k\pi}{f_\chi}\right|.$$

(b) 对于 n 次虚 Abel 数域 K，

$$R_{K_+}h_{K_+}=|d(K_+)|^{1/2}\prod_{\substack{\chi_0\neq\chi\in\hat{K}\\ \chi(-1)=1}}\frac{1}{\sqrt{f_\chi}}\left|\sum_{1<k<f_\chi/2}\chi(k)\log\sin\frac{k\pi}{f_\chi}\right|,$$

$$\begin{aligned}\frac{R_Kh_K}{R_{K_+}h_{K_+}}&=\frac{w_K}{2}|d(K)/d(K_+)|^{1/2}\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=-1}}\frac{1}{f_\chi^{3/2}}\left|\sum_{k=1}^{f_\chi-1}\chi(k)k\right|,\\&=\frac{w_K}{2}|d(K)/d(K_+)|^{1/2}\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=-1}}\frac{1}{\sqrt{f_\chi}|\chi(2)-2|}\\&\quad\cdot\left|\sum_{1<k<f_\chi/2}\chi(k)\right|.\end{aligned}$$

我们仍然可以将上面诸式右边作进一步化简．为此，我们需要第四章所介绍的 $L(s,\chi)$ 和 $\zeta_K(s)$ 的函数方程．它们可导出 $d(K)$ 和

f_χ之间一个简单而奇妙的关系，就是著名的 Hasse 判别式——导子公式.

引理 6(Hasse, 判别式——导子公式) 设 K 为 Abel 数域. 则

$$\prod_{\chi\in\widehat{K}} f_\chi = |d(K)|.$$

证明 将公式 $\zeta_K(s)=\prod_{\chi\in\widehat{K}} L(s,\ \chi^*)$ 两边的 D-级数均应用各自的函数方程. 由 $\zeta_K(s)$ 的函数方程不难算出，若令

$$\Phi_K(s)=\begin{cases}|d(K)|^{s/2}(\pi^{-s/2}\Gamma(s/2))^n\zeta_K(s), & \text{若 } K \text{ 为实域;}\\ |d(K)|^{s/2}(\pi^{-s/2}\Gamma(s/2))^{n/2}\left(\pi^{-s/2}\Gamma\left(\frac{1+s}{2}\right)\right)^{n/2} & \\ \quad\cdot\zeta_K(s), & \text{若 } K \text{ 为虚域.}\end{cases}$$

则 $|\Phi_K(s)|=|\Phi_K(1-s)|$. 这里我们使用了公式

$$\Gamma(s)=\Gamma(s/2)\Gamma\left(\frac{1+s}{2}\right)\cdot 2^{s-1}/\sqrt{\pi}.$$

另一方面，由 L-函数的函数方程可知，若令 χ 为模f_χ 的本原特征，而

$$\Phi(s,\ \chi)=\begin{cases}f_\chi^{s/2}(\pi^{-s/2}\Gamma(s/2))L(s,\ \chi), & \text{若 } \chi(-1)=1;\\ f_\chi^{s/2}\left(\pi^{-s/2}\Gamma\left(\frac{s+1}{2}\right)\right)L(s,\ \chi), & \text{若 } \chi(-1)=-1.\end{cases}$$

则 $|\Phi(s,\ \chi)|=|\Phi(1-s,\ \chi)|$. 现在由 $\zeta_K(s)=\prod_{\chi\in\widehat{K}} L(s,\ \chi^*)$ 即知

$$\left|\Phi_K(s)/\prod_{\chi\in\widehat{K}}\Phi(s,\ \chi)\right|=\left|d(K)/\prod_\chi f_\chi\right|^{s/2}.$$

但是左边将 s 改为 $1-s$ 时是不变的，于是右边也应如此. 但这只有 $|d(K)|=\prod_\chi f_\chi$ 的时候才可能. ∎

最后，将引理 6 和引理 5 放在一起，我们就给出 Hasse 于本世纪三十年代建立的.

定理 2 (Hasse, Abel 域类数解析公式)

(a) 若 K 为 n 次实 Abel 域，则

$$R_K h_K=\prod_{\chi_0\neq\chi\in\widehat{K}}\left|\sum_{1<k<f_\chi/2}\chi(k)\log\sin\frac{k\pi}{f_\chi}\right|.$$

(b) 若 K 为 n 次虚 Abel 域，则

$$R_{K_+}h_{K_+}=\prod_{\substack{\chi_0\neq\chi\in\hat{K}\\ \chi(-1)=1}}\left|\sum_{1<k<f_\chi/2}\chi(k)\log\sin\frac{k\pi}{f_\chi}\right|.$$

$$\frac{R_Kh_K}{R_{K_+}h_{K_+}}=\frac{w_K}{2}\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=-1}}\frac{1}{f_\chi}\left|\sum_{k=1}^{f_\chi-1}\chi(k)k\right|$$

$$=\frac{w_K}{2}\prod_{\substack{\chi\in\hat{K}\\ \chi(-1)=-1}}\frac{1}{|\chi(2)-2|}\left|\sum_{1<k<f_\chi/2}\chi(k)\right|. \qquad \blacksquare$$

在以下两小节里，我们要对于最早研究类数问题的两种数域——二次域和分圆域给出更简单的类数公式和进一步的结果与猜想。

§2 二次域的类数公式

根据上小节的理论，为了得到二次域 K 的类数公式，我们需要决定域 K 的特征群 $\hat{K}$。由于 $\mathrm{Gal}(K/\mathbb{Q})$ 为二元群，K 只有一个非平凡特征，我们暂时将它记为 $\lambda(\neq\chi_0)$。显然 $\lambda^2=\chi_0$。令 $K=\mathbb{Q}(\sqrt{d})$，d 无平方因子。我们已经证明了 $\mathrm{cond}(K)=|d(K)|$。因此 λ 可看作是模 $|d(K)|$ 的 D–特征。于是 $\zeta_K(s)=\zeta(s)\cdot L(s,\lambda^*)$。对于因子 $L(s,\lambda^*)$，我们需要知道

(a) λ 的导子 f_λ 是什么？

(b) 能否给出 D–特征 λ 的明显表达式？

问题(a)容易解决：利用判别式——导子公式(引理 6)，对于二次域 $K=\mathbb{Q}(\sqrt{d})$ 则为 $f_\lambda=|d(K)|$。因此 λ 应当是模 $|d(K)|$ 的本原特征，为了回答问题(b)，我们需要二次域中的素理想分解定律。如下定义 $\chi_K(p)$：

(i) 对于奇素数 p，令

$$\chi_K(p)=\begin{cases}\left(\dfrac{d(K)}{p}\right)=\left(\dfrac{d}{p}\right), & \text{如果 } p\nmid d;\\ 0, & \text{如果 } p\mid d.\end{cases}$$

(ii) $$\chi_K(2)=\begin{cases}1, & \text{若 } d\equiv1\pmod 8;\\ -1, & \text{若 } d\equiv5\pmod 8;\\ 0, & \text{否则.}\end{cases}$$

根据第二章所述，有理素数 p 在二次域 $K=\mathbb{Q}(\sqrt{d})$ 中分解规律为：

分歧：$p=\mathfrak{p}^2$，如果 $\chi_K(p)=0$（即 $p|d(K)$）；

完全分裂：$p=\mathfrak{p}_1\mathfrak{p}_2$，$\mathfrak{p}_1\neq\mathfrak{p}_2$，如果 $\chi_K(p)=1$；

惯性：$p=\mathfrak{p}$，如果 $\chi_K(p)=-1$。

现在我们将 χ_K 完全积性地将定义域扩充到全体自然数集合上。换句话说，如果 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，定义 $\chi_K(n)=\chi_K(p_1)^{\alpha_1}\cdots\chi_K(p_s)^{\alpha_s}$。由于 $|\chi_K(n)|=0$ 或者 1，从而 D-级数 $\sum\limits_{n=1}^{\infty}\chi_K(n)n^{-s}$ 在 $\mathrm{Re}(s)>1$ 中定义出正则函数，并且有 Euler 展开

$$\sum_{n=1}^{\infty}\chi_K(n)n^{-s}=\prod_p(1-\chi_K(p)p^{-s})^{-1}.\quad(\mathrm{Re}\,(s)>1).$$

引理 7 $\lambda=\chi_K$.

证明 我们已经知道 $\zeta_K(s)=\zeta(s)\sum\limits_{n=1}^{\infty}\lambda(n)n^{-s}$。根据 D-级数的唯一性定理，我们只需再证明 $\zeta_K(s)=\zeta(s)\sum\limits_{n=1}^{\infty}\chi_K(n)n^{-s}$ ($\mathrm{Re}\,(s)>1$) 即可。由于上式双方均有 Euler 乘积展开，从而只需对于每个有理素数 p 证明

$$\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s})=(1-p^{-s})(1-\chi_K(p)p^{-s})\qquad(*)$$

即可。事实上，

$$(*)\text{式左边}=\begin{cases}1-p^{-s} & (\text{若 } p \text{ 分歧})\\ (1-p^{-s})^2 & (\text{若 } p \text{ 完全分裂})\\ (1-p^{-2s}) & (\text{若 } p \text{ 惯性})\end{cases}$$

$$=\left.\begin{array}{l}(1-p^{-s})(1-0\cdot p^{-s})\\ (1-p^{-s})(1-p^{-s})\\ (1-p^{-s})(1-(-p^{-s}))\end{array}\right\}=(*)\text{式右边}.$$

于是证明了引理 7. ∎

现在很容易给出二次域的类数公式

定理 3

(a) 设 K 为虚二次域并且 $K\neq\mathbb{Q}(\sqrt{-1})$ 和 $\mathbb{Q}(\sqrt{-3})$，则

$$h_K = \frac{1}{|d(K)|}\sum_{k=1}^{|d(K)|}\chi_K(k)k$$

$$= \frac{1}{2-\chi_K(2)}\Big|\sum_{1<k<\frac{|d(K)|}{2}}\chi_K(k)\Big|.$$

(b) 对于实二次域 K，令 $\varepsilon>1$ 为 K 的基本单位，则

$$h_K = \frac{1}{\log\varepsilon}\Big|\sum_{1<k<\frac{|d(K)|}{2}}\chi_K(k)\log\sin\frac{\pi k}{|d(K)|}\Big|.$$

证明

(a) 对于虚二次域 $K=\mathbb{Q}(\sqrt{-d})$，$d>0$，$r=r_1+r_2-1=0$，从而 $R_K=1$．并且当 $|d(K)|>4$ 时，$w_K=2$．（对于 $|d(K)|\leqslant 3$，则 $K=\mathbb{Q}(\sqrt{-1})$ 和 $\mathbb{Q}(\sqrt{-3})$，我们在第三章中已经知道它们类数均为 1）．然后由定理 2 和引理 7 即得 (a) 中类数公式．

(b) 对于实二次域 K，$w_K=2$，$r=1$，$R_K=\log\varepsilon$，从而由定理 2 和引理 7 即得(b)中类数公式． ∎

例 1 $K=\mathbb{Q}(\sqrt{-5})$，$|d(K)|=20$，$\chi_K(2)=0$，χ_K 为模 20 的本原 D-特征．由 χ_K 的定义算出：$\chi_K(\text{偶数})=0$，$\chi_K(1)=\chi_K(9)=1$，$\chi_K(3)=\left(\frac{-5}{3}\right)=1$，$\chi_K(5)=0$，$\chi_K(7)=\left(\frac{-5}{7}\right)=1$．于是 $h_K=\frac{1}{2}|\chi(1)+\chi(3)+\chi(7)+\chi(9)|=2$．

例 2 $K=\mathbb{Q}(\sqrt{2})$，$|d(K)|=8$，$\chi_K(2)=0$，$\chi_K(1)=1$，$\chi_K(3)=-1$．基本单位为 $\varepsilon=1+\sqrt{2}$．于是

$$h_K = \frac{1}{\log(1+\sqrt{2})}\left|\chi(1)\log\sin\frac{\pi}{8}+\chi(3)\log\sin\frac{3\pi}{8}\right|$$

$$=\log\left(\frac{\sin\frac{3\pi}{8}}{\sin\frac{\pi}{8}}\right)\Big/\log(1+\sqrt{2}).$$

即 $$(1+\sqrt{2})^{h_K}=\sin\frac{3\pi}{8}\Big/\sin\frac{\pi}{8}=1+2\cos\frac{\pi}{4}=1+\sqrt{2},$$

从而 $h_K=1$．

在 Боревич 和 Шафаревич 的书“数论”(俄文，1964 年)中列出

了$\mathbb{Q}(\sqrt{-a})$, $1\leqslant a\leqslant 500$ 和 $\mathbb{Q}(\sqrt{d})$, $1\leqslant d\leqslant 500$ 的类数表. 下面是其中的一部分.

(I) 虚二次域 $\mathbb{Q}(\sqrt{-a})$, $1\leqslant a\leqslant 100$.

a	1	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23	26	29	30	31
h	1	1	1	2	2	1	2	1	2	4	2	4	1	4	2	3	6	6	4	3

a	33	34	35	37	38	39	41	42	43	46	47	51	53	55	57	58	59	61	62	65
h	4	4	2	2	6	4	8	4	1	4	5	2	6	4	4	2	3	6	8	8

a	66	67	69	70	71	73	74	77	78	79	82	83	85	86	87	89	91	93	94	95	97
h	8	1	8	4	7	4	10	8	4	5	4	3	4	10	6	12	2	4	8	8	4

(II) 实二次域 $\mathbb{Q}(\sqrt{d})$ $(2\leqslant d\leqslant 101)$. $\varepsilon>1$ 表示基本单位, $\omega=\dfrac{1+\sqrt{d}}{2}$(如果 $d\equiv 1\pmod 4$), $\omega=\sqrt{d}$ (如果 $d\equiv 2, 3\pmod 4$).

d	2	3	5	6	7	10	11	13	14	15	17
h	1	1	1	1	1	2	1	1	1	2	1
ε	$1+\omega$	$2+\omega$	ω	$5+2\omega$	$8+3\omega$	$3+\omega$	$10+3\omega$	$1+\omega$	$15+4\omega$	$4+\omega$	$3+2\omega$

d	19	21	22	23	26	29	30	31
h	1	1	1	1	2		2	1
ε	$170+39\omega$	$2+\omega$	$197+42\omega$	$24+5\omega$	$5+\omega$	$2+\omega$	$11+2\omega$	$1520+273\omega$

d	33	34	35	37	38	39	41	42
h	1	2	2	1	1	2	1	1
ε	$19+8\omega$	$35+6\omega$	$6+\omega$	$5+2\omega$	$37+6\omega$	$25+4\omega$	$27+10\omega$	$13+2\omega$

d	43	46	47	51	53	55	57
h	1	1	1	2			
ε	$2482+531\omega$	$24335+3588\omega$	$48+7\omega$	$50+7\omega$	$3+\omega$	$89+12\omega$	$131+40\omega$

d	58	59	61	62	65	66	67
h							1
ε	$99+13\omega$	$530+69\omega$	$17+5\omega$	$63+8\omega$	$7+2\omega$	$65+8\omega$	$48842+5967\omega$

d	69	70	71	73	74	77	78
h	1	2	1	1	1	1	2
ε	$11+3\omega$	$251+30\omega$	$3480+413\omega$	$943+250\omega$	$43+5\omega$	$4+\omega$	$53+6\omega$

d	79	82	83	85	86	87	89
h	3	4	1	2	1	2	1
ε	$80+9\omega$	$9+\omega$	$82+9\omega$	$4+\omega$	$10405+1122\omega$	$28+3\omega$	$447+106\omega$

d	91	93	94	95	97	101
h	2	1	1	2	1	1
ε	$1574+165\omega$	$13+2\omega$	$2143295+221064\omega$	$39+4\omega$	$5035+1138\omega$	$9+2\omega$

利用二次域的类数公式，我们可以对类数的下界给出一些估计(习题 6)．关于二次域的类数问题，Gauss 有两个著名的猜想：

(1) 只有有限多个虚二次域类数为 1；

(2) 存在着无限多个类数为 1 的实二次域．

关于猜想(1)， Gauss 本人计算出当 $K=\mathbb{Q}(\sqrt{-d})$，$d=1, 2, 3, 7, 11, 19, 43, 67$ 和 163 时，$h_K=1$．他预言只有这九个虚二次域的类数为 1．1934 年，Heilbronn 证明了猜想(1)，确切地说，Heilbronn 证明了：当 $d>163$ 时至多还有一个虚二次域类数为 1．至于这个例外的域是否存在，是一个长期未解决的问题．一直到 1967 年才由英国数学家 Baker 和美国数学家 Stark 独立地解决：那个例外的域是不存在的．换句话说，类数为 1 的虚二次域只有 Gauss 发现的那 9 个．另一方面，关于 Gauss 猜想(2)，人们至今未能解决．实二次域比虚二次域类数问题要困难，其主要原因是类数公式中多了一个因子 $\log\varepsilon$．

关于二次域类数的估计问题，对于实二次域

$$K=\mathbb{Q}(\sqrt{d}) \quad (d>0),$$

华罗庚证明了 $h_K<\sqrt{d}$. 这个结果本质上已是最好的可能, 因为在另一方面, 人们证明了: 对于每个 $\varepsilon>0$, 均存在无限多个实二次域 $K=\mathbb{Q}(\sqrt{d})$ 使得 $h_K>d^{\frac{1}{2}-\varepsilon}$. 对于虚二次域 $K=\mathbb{Q}(\sqrt{d})$ $(d<0)$, 类似地证明了当 $|d|>e^{24}$ 时, $h_K\leqslant\frac{1}{3}|d|^{1/2}\log|d|$. 并且对每个 $\varepsilon>0$, 当 $|d|$ 充分大时, 均有 $h_K>|d|^{1/2-\varepsilon}$.

§3 分圆域的类数公式, Kummer 结果

我们已经说过多次, 在历史上是 Kummer 研究 Fermat 猜想导致对分圆域的类数作深入的研究, 这是代数数论的一个重要的源头. Kummer 关于分圆域类数问题的最主要研究结果为

(I) 以 h_p 表示分圆域 $\mathbb{Q}(\zeta_p)$ 的类数 (p 为奇素数). 如果 $p\nmid h_p$, 则 Fermat 方程 $x^p+y^p=z^p$ 没有非平凡的有理整数解.

(II) 以 h_p^+ 表示 $\mathbb{Q}(\zeta_p)$ 的极大实子域 $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ 的类数. 则 $h_p^+|h_p$. 整数 h_p^+ 和 $h_p^-=h_p/h_p^+$ 分别叫作是类数 h_p 的第二因子和第一因子.

(III) $p|h_p\Leftrightarrow p|h_p^-\Leftrightarrow p$ 至少除尽 Bernoulli 数 $B_2, B_4, \cdots, B_{p-3}$ 中一个的分子.

我们在第三章的末尾已经谈到(I), 并且对于 Fermat 方程的第一种情形给出了证明. 本小节的目的是讲述(II)和(III), 这就依赖于分圆域的类数公式. 为了简单起见, 我们只考分圆域 $K=\mathbb{Q}(\zeta_p)$ (p 为奇素数). 这时 $w_K=2p$. 于是由定理 2 给出.

定理 4 设 h_p 和 p_p^+ 分别是 $\mathbb{Q}(\zeta_p)$ 和 $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ 的类数, R_p 和 R_p^+ 分别是它们的 regulator. 则

(a) $$R_p^+h_p^+=\prod_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}}\left|\sum_{k=1}^{(p-1)/2}\chi(k)\log\sin\frac{k\pi}{p}\right|,$$

其中 χ 过模 p 的 $\frac{p-3}{2}$ 个非主偶特征.

(b) $$\frac{R_p h_p}{R_p^+ h_p^+} = p^{-\frac{p-3}{2}} \prod_{\chi(-1)=-1} \left| \sum_{k=1}^{p-1} \chi(k) k \right|$$
$$= p \prod_{\chi(-1)=-1} \frac{1}{|\chi(2)-2|} \left| \sum_{k=1}^{(p-1)/2} \chi(k) \right|$$
其中 χ 过模 p 的 $\frac{p-1}{2}$ 个奇特征. ∎

我们在第三章证明了 $R_p = R_p^+ \cdot 2^{\frac{p-3}{2}}$, 从而由定理 4 的(b)立刻得到

系 $$h_p^- = (2p)^{-\frac{p-3}{2}} \prod_{\chi(-1)=-1} \left| \sum_{k=1}^{p-1} \chi(k) k \right|$$
$$= 2^{-\frac{p-3}{2}} \cdot p \prod_{\chi(-1)=-1} \left(\frac{1}{|\chi(2)-2|} \left| \sum_{k=1}^{(p-1)/2} \chi(k) \right| \right).$$

现在我们用类数公式证明

定理 5 $h_p^- \in \mathbb{Z}$.

证明 模 p 的 $p-1$ 个 D-特征形成一个循环群, 其生成元为 χ, $\chi(g^t) = \zeta_{p-1}^t (0 \leqslant t \leqslant p-2)$, 其中 g 是模 p 的一个原根. 于是, 模 p 的全部奇特征为 $\left\{ \chi^{2l+1} \mid 0 \leqslant l \leqslant \frac{p-3}{2} \right\}$. 特别地, $\prod_{k=1}^{p-1} \chi(k) k$ 均是分圆域 $\mathbb{Q}(\zeta_{p-1})$ 中的整数, 从而

$$B = \prod_{\chi(-1)=-1} \sum_{k=1}^{p-1} \chi(k) k$$

也是 $\mathbb{Q}(\zeta_{p-1})$ 中整数, 即 $B \in \mathbb{Z}[\zeta_{p-1}]$. 如果我们能够证明 $(2p)^{\frac{p-3}{2}} \mid B$, 则 $(2p)^{-\frac{p-3}{2}} B$ 为整数. 但是

$$(2p)^{-\frac{p-3}{2}} B = \pm h_p^- = \pm h_p / h_p^+ \in \mathbb{Q}.$$

这就表明 $h_p / h_p^+ \in \mathbb{Z}$, 即 $h_p^- \in \mathbb{Z}$. 因此我们只需证明在 $\mathbb{Z}[\zeta_{p-1}]$ 中 $(2p)^{\frac{p-3}{2}} \mid B$ 即可.

以 g_s 表示 g^s 对于模 p 的最小正剩余. 则

$$\sum_{k=1}^{p-1} \chi^{2l+1}(k) k = \sum_{s=0}^{p-2} \chi^{2l+1}(g^s)^{-1} g_s = \sum_{s=0}^{p-2} g_s \zeta_{p-1}^{(2l+1)s} = F(\zeta_{p-1}^{2l+1}),$$

其中 $$F(x) = \sum_{s=0}^{p-2} g_s x^s \in \mathbb{Z}[x].$$

于是 $$B = F(\zeta_{p-1}) F(\zeta_{p-1}^3) \cdots F(\zeta_{p-1}^{p-2}).$$

我们现在分两步证明$(2p)^{\frac{p-3}{2}}|B$.

(I) **证明$2^{\frac{p-3}{2}}|B$**：当$2\nmid k$时，在$\mathbb{Q}(\zeta_{p-1})$中

$$
\begin{aligned}
F(\zeta_{p-1}^k) &= \sum_{s=0}^{(p-3)/2}\left(g_s\zeta_{p-1}^{ks}+g_{\frac{p-1}{2}+s}\,\zeta_{p-1}^{k\left(\frac{p-1}{2}+s\right)}\right)\\
&= \sum_{s=0}^{(p-3)/2}\left(g_s-g_{\frac{p-1}{2}+s}\right)\zeta_{p-1}^{ks}\\
&= \sum_{s=0}^{(p-3)/2}\zeta_{p-1}^{ks}(g_s-(p-g_s))\\
&\equiv \sum_{s=0}^{(p-3)/2}\zeta_{p-1}^{ks} \pmod 2.
\end{aligned}
$$

从而

$$
\begin{aligned}
F(\zeta_{p-1}^k)(1-\zeta_{p-1}^k) &\equiv \sum_{s=0}^{(p-3)/2}\zeta_{p-1}^{ks}(1-\zeta_{p-1}^k)\\
&=1-\zeta_{p-1}^{k\cdot\frac{p-1}{2}}=2\equiv 0 \pmod 2.
\end{aligned}
$$

于是

$$
\begin{aligned}
2^{\frac{p-1}{2}}&\Big|\prod_{s=0}^{(p-3)/2}F(\zeta_{p-1}^{2s+1})(1-\zeta_{p-1}^{2s+1})\\
&=B(1-\zeta_{p-1})(1-\zeta_{p-1}^3)\cdots(1-\zeta_{p-1}^{p-2}).
\end{aligned}
$$

但是
$$\prod_{k=1}^{p-2}(1-\zeta_{p-1}^k)=(x^{p-1}-1)'|_{x=1}=p-1;$$

$$\prod_{k=1}^{(p-3)/2}(1-\zeta_{p-1}^{2k})=\prod_{s=0}^{(p-3)/2}(1-\zeta_{\frac{p-1}{2}}^k)=(x^{\frac{p-1}{2}}-1)'|_{x=1}=\frac{p-1}{2}.$$

从而$(1-\zeta_{p-1})(1-\zeta_{p-1}^3)\cdots(1-\zeta_{p-1}^{p-2})=(p-1)\Big/\frac{p-1}{2}=2$，这就证明了$2^{\frac{p-3}{2}}|B$.

(II) **证明$p^{\frac{p-3}{2}}|B$**：我们需要考虑p在分圆域$\mathbb{Q}(\zeta_{p-1})$中的素理想分解．由于p对于模$(p-1)$的阶为1．从而由分圆域中素理想分解规律(第二章)可知p在$K=\mathbb{Q}(\zeta_{p-1})$中完全分裂．即

$$pO_K=\mathfrak{p}_1\cdots\mathfrak{p}_g,\quad g=\varphi(p-1).$$

取$\mathfrak{p}=\mathfrak{p}_i$．则

(a) $0, 1, \zeta_{p-1}, \cdots, \zeta_{p-1}^{p-2}$两两模$\mathfrak{p}$不同余(若$\zeta_{p-1}^i-\zeta_{p-1}^j\in\mathfrak{p}$,

$0\leqslant i<j\leqslant p-2$，则 $1-\zeta_{p-1}^{j-i}\in\mathfrak{p}$．但是 $\sum\limits_{k=1}^{p-2}(1-\zeta_{p-1}^{k})=p-1$，于是 $p-1\in\mathfrak{p}|p$，这显然不可能）．由于 $N(\mathfrak{p})=p^f=p$，从而 $\{0,1,\zeta_{p-1},\zeta_{p-1}^2,\cdots,\zeta_{p-1}^{p-2}\}$ 就是 $\mathbb{Z}[\zeta_{p-1}]$ 模 $\mathfrak{p}$ 的完全代表系．

(b) $1-\zeta_{p-1}^k g\in\mathfrak{p}_i$（对某个 i，$1\leqslant i\leqslant r$）$\Leftrightarrow(k,p-1)=1$．

这是因为：由于 $0\equiv1-g^{p-1}=\prod\limits_{k=1}^{p-2}(1-\zeta_{p-1}^k g)\pmod p$，从而对于每个 $\mathfrak{p}|p$，均有一个 $1-\zeta_{p-1}^k g$ 使得 $1-\zeta_{p-1}^k g\in\mathfrak{p}$．根据 (a) 可知，对于每个固定的 $\mathfrak{p}$，也只有一个这样的 $1-\zeta_{p-1}^k g$．进而，若 $(k,p-1)=d$，则

$$
\begin{aligned}
1\equiv\zeta_{p-1}^k g\pmod{\mathfrak{p}}&\Rightarrow\mathfrak{p}\,|\,g^{\frac{p-1}{d}}-1\Rightarrow p\,|\,g^{\frac{p-1}{d}}-1\\
&\Rightarrow p-1\,\Big|\,\frac{p-1}{d}\Rightarrow d=1.
\end{aligned}
$$

从而若 $1-\zeta_{p-1}^k g\in\mathfrak{p}$，则必然 $(k,p-1)=1$．但是满足 $(k,p-1)=1$，$1\leqslant k\leqslant p-1$ 的 $1-\zeta_{p-1}^k g$ 共有 $\varphi(p-1)$ 个，而 $\mathfrak{p}_i$ 也是 $\varphi(p-1)=g$ 个．这就表明对于每个 $(k,p-1)=1$ 的 k，均恰好有 p 在 $\mathbb{Q}(\zeta_{p-1})$ 中的一个素理想因子 $\mathfrak{p}$，使得 $1-\zeta_{p-1}^k g\in\mathfrak{p}$．我们不妨对 p 的素理想因子重新加以标记，使得

$$
(p)=\prod_{\substack{1\leqslant k\leqslant p-1\\(k,p-1)=1}}\mathfrak{p}_k\quad \mathfrak{p}_k\,|\,(1-\zeta_{p-1}^k g).
$$

现在回到我们的问题上来，即要证 $p^{\frac{p-3}{2}}|B$．在 $\mathbb{Z}[\zeta_{p-1}]$ 中，

$$
\begin{aligned}
F(\zeta_{p-1}^k)(1-g\zeta_{p-1}^k)&\equiv\sum_{s=0}^{p-2}(g\zeta_{p-1}^k)^s(1-g\zeta_{p-1}^k)\\
&=1-(g\zeta_{p-1}^k)^{p-1}\equiv1-g^{p-1}\\
&\equiv0\pmod p.
\end{aligned}
$$

当 $(k,p-1)>1$ 时，由 (b) 知对每个 l，$(l,p-1)=1$，均有 $\mathfrak{p}_l\nmid(1-g\zeta_{p-1}^k)$．从而 $p|F(\zeta_{p-1}^k)$．而当 $(k,p-1)=1$ 时，如果 $(l,p-1)=1$，$l\neq k$，则也有 $\mathfrak{p}_l\nmid(1-g\zeta_{p-1}^k)$．于是

$$
p\mathfrak{p}_k^{-1}=\prod_{\substack{1\leqslant l\leqslant p-1\\(l,p-1)=1\\l\neq k}}\mathfrak{p}_l\,|\,F(\zeta_{p-1}^k).
$$

从而 $B=F(\zeta_{p-1})F(\zeta_{p-1}^2)\cdots F(\zeta_{p-1}^{p-2})$ 可被

$$p^{\frac{p-1}{2}}\prod_{(k,p-1)=1}\mathfrak{p}_k^{-1}=p^{\frac{p-3}{2}}$$

除尽. 这就完全证明了定理 5. ∎

为了介绍 Kummer 结果(III), 我们需要关于 Bernoulli 数的一些重要的性质. 我们在第四章中给出了 Bernoulli 数 B_n, 广义 Bernoulli 数 $B_{n,\chi}$ 和 Bernoulli 多项式 $B_n(x)$ 的定义. 它们之间有如下的关系:

$$B_n(x)=\sum_{i=0}^{\infty}\binom{n}{i}B_i x^{n-i},$$

$$B_{n,\chi}=f^{n-1}\sum_{a=1}^{f}\chi(a)B_n\left(\frac{a}{f}\right)\quad(\chi\text{ 为模 }f\text{ 的 D-特征}),$$

$$B_n=B_{n,\chi_0}\quad(\text{当 }n\geqslant 2\text{ 时}).$$

引理 8 设 χ 为模 f 的 D-特征.

(a) 对于每个正整数 $F\equiv 0\pmod f$, 均有

$$B_{n,\chi}=F^{n-1}\sum_{a=1}^{F}\chi(a)B_n\left(\frac{a}{F}\right).$$

(b) (von Staudt-Clausen) 设 n 为正偶数, 则

$$B_n+\sum_{p-1\mid n}\frac{1}{p}\in\mathbb{Z}.$$

(c) 设 n 为正偶数并且 $n\leqslant p-3$, (p 为奇素数), 则

$$\sum_{a=1}^{p-1}a^n\equiv pB_n\pmod{p^2}.$$

证明

(a) 根据定义我们有

$$\sum_{n=0}^{\infty}B_n(x)\frac{t^n}{n!}=\frac{te^{xt}}{e^t-1},\qquad\sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!}=\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1},$$

从而

$$\begin{aligned}&\sum_{n=0}^{\infty}F^{n-1}\sum_{a=1}^{F}\chi(a)B_n\left(\frac{a}{F}\right)\frac{t^n}{n!}\\&=\sum_{a=1}^{F}\chi(a)\frac{te^{(a/F)Ft}}{e^{Ft}-1}=\sum_{b=1}^{f}\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf)t}}{e^{Ft}-1}\\&=\sum_{b=1}^{f}\chi(b)\frac{te^{bt}}{e^{ft}-1}=\sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!},\end{aligned}$$

由此即得(a).

(b) 我们只需证明：对每个素数 p 均有

$p\nmid pB_n$ 的分母，并且

$$pB_n \equiv \begin{cases} -1, \pmod p, & \text{当 } p-1 \mid n \text{ 时;} \\ 0, \pmod p, & \text{当 } p-1 \nmid n \text{ 时.} \end{cases} \tag{*}$$

设 $n=2m$. 当 $m=1$ 时，$B_2=\frac{1}{6}=1-\frac{1}{2}-\frac{1}{3}$，易知(*)式对于 $m=1$ 成立. 现在对 m 归纳. 假设(*)式对于 $n=2, 4, \cdots, 2m-2$ 均成立，由本引理的(a)($f=1$, $F=p$)，我们有

$$pB_{2m}=pB_{2m,\chi_0}=p^{2m}\sum_{a=1}^{p} B_{2m}\left(\frac{a}{p}\right)$$

$$=p^{2m}\sum_{a=1}^{p}\sum_{j=0}^{2m}\binom{2m}{j}B_j\cdot\left(\frac{a}{p}\right)^{2m-j}$$

$$=\sum_{a=1}^{p}\sum_{j=0}^{2m}\binom{2m}{j}(pB_j)a^{2m-j}p^{j-1} \quad \text{(再利用归纳假设)}$$

$$\equiv\sum_{a=1}^{p}(pB_0a^{2m}p^{-1}+2mpB_1a^{2m-1}+pB_{2m}p^{2m-1}) \pmod p$$

由于 $B_0=1$, $B_1=-\frac{1}{2}$, $2mpB_1=-mp\equiv 0 \pmod p$，于是由上式可知

$$(1-p^{2m-1})pB_{2m}\equiv\sum_{a=1}^{p}a^{2m}$$

$$\equiv\begin{cases} p-1, \pmod p, & \text{若 } (p-1)\mid 2m; \\ 0 \quad \pmod p, & \text{若 } (p-1)\nmid 2m. \end{cases}$$

由于 $1-p^{2m-1}\equiv 1 \pmod p$，这就表明 $pB_{2m}\in\mathbb{Z}/p\mathbb{Z}$，并且

$$pB_{2m}\equiv\begin{cases} -1 \pmod p, & \text{若 } (p-1)\mid 2m; \\ 0 \pmod p, & \text{若 } (p-1)\nmid 2m. \end{cases}$$

(c) 因为

$$\sum_{n=0}^{\infty}(B_n(k)-B_n(0))\frac{t^n}{n!}=\frac{t(e^{kt}-1)}{e^t-1}=t(1+e^t+e^{2t}+\cdots+e^{(k-1)t})$$

$$=t+t\sum_{n=0}^{\infty}(1+2^n+\cdots+(k-1)^n)\frac{t^n}{n!}$$

从而当 $n, k\geqslant 1$ 时，

$$\sum_{a=1}^{k-1} a^n=\frac{1}{n+1}(B_{n+1}(k)-B_{n+1}(0))$$
$$=\frac{1}{n+1}(B_{n+1}(k)-B_{n+1})。$$

从而

$$\sum_{a=1}^{p-1} a^n=\frac{1}{n+1}(B_{n+1}(p)-B_{n+1})$$
$$=\frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k}B_k p^{n+1-k}$$
$$\equiv\frac{1}{n+1}\binom{n+1}{n}B_n p \pmod{p^2}$$
$$\equiv pB_n \pmod{p^2}。 \quad ∎$$

现在我们讲述 Kummer 的结果(III)。

定理6 $p|h_p^-\Leftrightarrow$ 存在 $k\in\{2, 4, \cdots, p-3\}$，使得 p 除尽 B_K 的分子.

证明 我们在定理5的证明中曾经得到如下的理想恒等式：

$$(h_p^-)=\left(\frac{B}{p^{(p-3)/2}}\right)=\prod_{k=1,3,\cdots,p-2}\frac{F(\zeta_{p-1}^k)\mathfrak{p}_k}{p}$$

(其中 $(k, p-1)>1$ 时规定 $\mathfrak{p}_k=1$)。

于是

$$p|h_p^-=\pm B/p^{(p-3)/2}\Leftrightarrow \mathfrak{p}_{p-2}|p^{-(p-3)/2}B$$

$\Leftrightarrow$ 存在 $k\in\{1, 3, \cdots, p-2\}$ 使得

$$\mathfrak{p}_{p-2}|F(\zeta_{p-1}^k)\mathfrak{p}_k p^{-1}$$

(因为 $F(\zeta_{p-1}^k)\mathfrak{p}_k p^{-1}$ 为整理想)。

$\Leftrightarrow$ 存在 $k\in\{1, 3, \cdots, p-2\}$，使得

$$\mathfrak{p}_{p-2}^2|F(\zeta_{p-1}^k)\mathfrak{p}_k.$$

$\Leftrightarrow$ 存在 $k\in\{1, 3, \cdots, p-4\}$，使得

$$\mathfrak{p}_{p-2}^2|F(\zeta_{p-1}^k) \qquad (1)$$

最后一式是因为 $\zeta_{p-1}^{p-2}g\equiv 1 \pmod{\mathfrak{p}_{p-2}}$，从而

$$F(\zeta_{p-1}^{p-2}) \equiv \sum_{s=0}^{p-2} (\zeta_{p-1}^{p-2} g)^s \equiv p-1 \equiv -1 \pmod{\mathfrak{p}_{p-2}},$$

因此 $\mathfrak{p}_{p-2}^2 \nmid F(\zeta_{p-1}^{p-2}) \mathfrak{p}_{p-2}$.

现在我们取模 p 原根 g, 使得 $g^{p-1} \equiv 1 \pmod{p^2}$ (设 g_0 为模 p 任一原根, 则 $g_0 + lp (l \in \mathbb{Z})$ 均为模 p 原根. 取 l 使得 $g_0^{p-2} l \equiv \frac{g_0^{p-1}-1}{p}$ $\pmod{p}$, 则 $g = g_0 + lp$ 即为所求)。这时

$$0 \equiv 1 - g^{p-1} = \prod_{k=0}^{p-2} (1 - \zeta_{p-1}^k g) \pmod{p^2}.$$

与定理5证明中所作的一样, 可以得到: 当 $(k, p-1) = 1$ 时, $\mathfrak{p}_k^2 | 1 - \zeta_{p-1}^k g$. 特别取 $k = p-2$, 则 $\zeta_{p-1} \equiv g \pmod{\mathfrak{p}_{p-2}^2}$. 于是

$$F(\zeta_{p-1}^k) = \sum_{s=0}^{p-2} g_s \zeta_{p-1}^{sk} \equiv \sum_{s=0}^{p-2} g_s g^{sk} \pmod{\mathfrak{p}_{p-2}^2}.$$

从而

$$\mathfrak{p}_{p-2}^2 | F(\zeta_{p-1}^k) \Leftrightarrow \sum_{s=0}^{p-2} g_s g^{sk} \equiv 0 \pmod{p^2} \tag{2}$$

但是 $g_s \equiv g^s + pa_s \pmod{p^2}$, $0 \leqslant s \leqslant p-2$, $a_s \in \mathbb{Z}$. 升到 $k+1$ 次幂 $(k=1, 3, \cdots, p-4)$, 则

$$\begin{aligned} g_s^{k+1} &\equiv g^{(k+1)s} + (k+1) g^{sk} p a_s \equiv g^{s(k+1)} + (k+1) g^{sk} (g_s - g^s) \\ &\equiv (k+1) g_s g^{sk} - k g^{s(k+1)} \pmod{p^2} \end{aligned} \tag{3}$$

由于 $k+1 \leqslant p-3$, 因此 $g^{k+1} \not\equiv 1 \pmod{p}$ 而 $g^{p-1} \equiv 1 \pmod{p^2}$, 从而

$$\sum_{s=0}^{p-2} g^{s(k+1)} = g^{(p-1)(k+1)} - 1 / g^{k+1} - 1 \equiv 0 \pmod{p^2}.$$

于是由(3)式可知

$$\sum_{n=1}^{p-1} n^{k+1} = \sum_{s=0}^{p-2} g_s^{k+1} \equiv (k+1) \sum_{s=0}^{p-2} g_s g^{sk} \pmod{p^2}.$$

再由(1)和(2)式即知

$$p | h_p^- \Leftrightarrow \text{存在 } k \in \{2, 4, \cdots, p-3\}, \text{使得 } p^2 | \sum_{n=1}^{p-1} n^k.$$

但是由引理8知道 $p \nmid B_k$ 的分母 (因为 $k \leqslant p-3$, $(p-1) \nmid k$) 并且 $\sum_{n=1}^{p-1} n^k \equiv pB_k \pmod{p^2}$, 从而 $p^2 | \sum_{n=1}^{p-1} n^k \Leftrightarrow p | B_k$ 的分子。这就给出最后结果:

$p|h_p^- \Leftrightarrow$ 存在 $k\in\{2, 4, \cdots, p-3\}$, 使得 $p|B_k$ 的分子. ∎

注记

1. 定理6相当于Kummer结果(III)的一半. 另一半是 $p|h_p^- \Leftrightarrow p|h_p = h_p^- h_p^+$, 这相当于说: $p|h_p^+ \Rightarrow p|h_p^-$. 为了证明这一点我们需要局部域的进一步的知识, 这里就不介绍了. 事实上Vandiver猜想: 对每个奇素数 p 均有 $p\nmid h_p^+$. 这个猜想对于 $p<125000$ 均已验证是对的. 但是目前人们还不清楚对于每个奇素数 p 这是否均成立.

2. 如果 $p\nmid h_p$(即 $p\nmid h_p^-$), Kummer称这种 p 为正规素数. 而当 $p|h_p$ 时称 p 为不正规素数. Kummer本人计算了在100以内只有3个不正规素数: $p=37$, 59和67. 从Fermat猜想的角度看(p 正规则 $x^p+y^p=z^p$ 无非平凡整数解), 自然希望正规素数愈多愈好. 但是目前人们反而证明了不正规素数有无穷多个, 而正规素数是否有无穷多个, 现在既没有被肯定也没有被否定. 虽然通过大量的计算(Wagstaff于1978年计算出125000以内的全部不正规素数)人们倾向于认为正规素数也有无穷多个, 甚至于从概率论上的考虑, 猜想: 正规素数和不正规素数的比例分别各占 $e^{-1/2}\approx 61\%$ 和 $1-e^{-1/2}\approx 39\%$.

3. Kummer当年通过手算发现: 当 $p\to+\infty$ 时, h_p^+ 增长较慢, 但是 h_p^- 增长飞快. 由于 $h_p=h_p^+h_p^-$, 自然会提出如下的问题:

(A) 类数为1的分圆域是否只有有限多个?

(B) 当 $p\to+\infty$ 时, h_p^+ 和 h_p^- 的性状如何?

1976年, Masley和Montgomery完全解决了问题(A). 他们证明了: 分圆域 $\mathbb{Q}(\zeta_m)$ 的类数 $h_m=1 \Leftrightarrow m=3$, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84 (共29个). 证明中综合性地利用了代数工具和解析工具. Washington将证明作了更好的整理, 写成书"Introduction to Cyclotomic Fields"的第11章. 差不多与此同时, Masley(1976年)决定出 $h_m\leqslant 10751$ 的全部 m(!). 如 $h_m=2 \Leftrightarrow m=39$, 56; $h_m=3 \Leftrightarrow m=23$, 52, 72等等.

至于问题(B)，关于 h_p^+ 的性状是一个很难的数论问题. 其困难主要来自于很难求 $\mathbb{Q}(\zeta_p)$ 的基本单位系，从而不知道 Regulator 值. 目前人们甚至猜不出 h_p^+ ($p\to+\infty$ 时)的发展规律. Masley 猜想 $h_p^+<p$，但是 1982 年 Washington 在广义 Riemann 猜想之下证明了对于 $p=11290018777$，这个猜想是不对的. 对于 h_p^-，Kummer 有如下一个著名猜想:

$$h_p^-\sim 2p\left(\frac{p}{4\pi^2}\right)^{\frac{p-1}{4}}=2p\left(\frac{p}{39.4784\cdots}\right)^{\frac{p-1}{4}}\quad(\text{当 } p\to+\infty \text{ 时}).$$

这一猜想至今未能证明. 如果令 $G_p=2p\left(\frac{p}{4\pi^2}\right)^{\frac{p-1}{4}}$，目前只能证明到下面的结果:

$$\frac{2}{3}<\frac{h_p^-}{G_p}<\frac{3}{2}\quad(\text{当 } 5\leqslant p\leqslant 523).$$

$$\frac{e^{-12.93}}{Lp^{\frac{1}{2}}(\lg p)^4}<\frac{h_p^-}{G_p}<e^{15.49}L(\lg p)^5$$

$$(\text{对任意 } p),\ (L=e^{4.66/\lg p})\cdots\qquad(*)$$

从 h_p^- 的解析公式和引理 5 我们知道

$$h_p^-=2p\prod_{\chi(-1)=-1}\left(\frac{-1}{2p}\sum_{a=1}^{p-1}a\chi(a)\right)$$

$$=2p\left(\frac{p}{4\pi^2}\right)^{\frac{p-1}{4}}\prod_{\chi(-1)=-1}L(1,\ \chi).$$

从而 Kummer 猜想等价于

$$\prod_{\chi(-1)=-1}L(1,\ \chi)\sim 1$$

$$\left(\text{当 } p\to\infty \text{ 时. 这里 } \chi \text{ 过 } \frac{p-1}{2} \text{ 个模 } p \text{ 奇特征}\right).$$

对于 $L(1,\chi)$ 运用相当深刻的解析工具，才能证到象(*)那样的结果. 另一方面，从 h_p^- 的解析公式出发采用很初等的方法，Carlitz 于 1961 年证明了 $h_p^-\leqslant(p-1)\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}$. Metsänkyla 于 1974 年又将其改进为 $h_p^-\leqslant 2p\left(\frac{(p-1)(p-2)}{24p}\right)^{\frac{p-1}{4}}$. 作为本书的结束，

我们现在进一步证明出 $h_p^-\leqslant 2p\left(\frac{p-1}{31.997158\cdots}\right)^{\frac{p-1}{4}}$. 证明是初等的. 事实上我们有

引理 9 设 l 是 2 模 p 的阶数(即满足 $2^l\equiv 1\pmod p$ 的最小正整数)则

$$h_p^-\leqslant\begin{cases}2p\left(\frac{p-1}{8(2^{l/2}+1)^{4/l}}\right)^{\frac{p-1}{4}}, & \text{当 } 2|l \text{ 时;}\\ 2p\left(\frac{p-1}{8(2^l-1)^{2/l}}\right)^{\frac{p-1}{4}}, & \text{当 } 2\nmid l \text{ 时.}\end{cases}$$

证明 从解析类数公式出发(定理 4)

$$h_p^-=2^{-\frac{p-3}{2}}p\prod_{\chi(-1)=-1}\frac{1}{|\chi(2)-2|}\prod_{\chi(-1)=-1}\left|\sum_{a=1}^{(p-1)/2}\chi(a)\right| \tag{1}$$

其中 χ 过模 p 的 $\frac{p-1}{2}$ 个奇特征. 先计算第一个乘积. 由于 2 在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中的阶数是 l, 因此当 χ 过模 p 的全部 $\frac{p-1}{2}$ 个特征时,

$$\prod_{\chi}(2-\chi(2))=\prod_{i=1}^{p-1}(2-\zeta_l^i)=\left(\prod_{i=0}^{l-1}(2-\zeta_l^i)\right)^{\frac{p-1}{l}}$$
$$=(2^l-1)^{\frac{p-1}{l}}.$$

而 2 在商群 $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ 中的阶为 $l/2$ (当 $2|l$ 时) 或者 l(当 $2\nmid l$ 时), 因此$\Big($注意$(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$的特征群即是 $\frac{p-1}{2}$ 个模 p 偶特征$\Big)$.

$$\prod_{\chi(-1)=1}(2-\chi(2))=\begin{cases}(2^{l/2}-1)^{\frac{p-1}{l}}, & \text{当 } 2|l \text{ 时;}\\ (2^l-1)^{\frac{p-1}{2l}}, & \text{当 } 2\nmid l \text{ 时.}\end{cases}$$

从而

$$\prod_{\chi(-1)=-1}\left|\frac{1}{\chi(2)-2}\right|=\begin{cases}(2^{l/2}+1)^{-\frac{p-1}{l}}, & \text{当 } 2|l \text{ 时;}\\ (2^l-1)^{-\frac{p-1}{2l}}, & \text{当 } 2\nmid l \text{ 时.}\end{cases} \tag{2}$$

对于(1)中第 2 个乘积, 由几何平均值≤算术平均值, 我们有

$$\prod_{\chi(-1)=-1}\left|\sum_{a=1}^{\frac{p-1}{2}}\chi(a)\right|^{\frac{4}{p-1}}=\prod_{\chi(-1)=-1}\left(\sum_{a,b=1}^{(p-1)/2}\chi(a)\overline{\chi}(b)\right)^{\frac{2}{p-1}}$$

$$\leqslant\frac{2}{p-1}\sum_{\chi(-1)=-1}\sum_{a,b=1}^{(p-1)/2}\chi(a/b)$$

$$=\frac{2}{p-1}\sum_{a,b=1}^{\frac{p-1}{2}}\sum_{\chi(-1)=-1}\chi(a/b).$$

但是由特征之间的正交关系易知

$$\sum_{\chi(-1)=-1}\chi(a/b)=\begin{cases}\dfrac{p-1}{2}, & 若\ a\equiv b\ (\bmod p);\\ -\dfrac{p-1}{2}, & 若\ a\equiv -b\ (\bmod p);\\ 0, & 否则\end{cases}$$

于是

$$\prod_{\chi(-1)=-1}\left|\sum_{a=1}^{(p-1)/2}\chi(a)\right|^{4/(p-1)}\leqslant\frac{2}{p-1}\cdot\frac{p-1}{2}\cdot\frac{p-1}{2}=\frac{p-1}{2},$$

即

$$\prod_{\chi(-1)=-1}\left|\sum_{a=1}^{(p-1)/2}\chi(a)\right|\leqslant\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}} \tag{3}$$

将(2)和(3)式代入(1)式，即知当 $2|l$ 时，

$$h_p^-\leqslant 2^{-\frac{p-3}{2}}p(2^{l/2}+1)^{-\frac{p-1}{l}}\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}$$

$$=2p\left(\frac{p-1}{8(2^{l/2}+1)^{4/l}}\right)^{\frac{p-1}{4}},$$

而当 $2\nmid l$ 时，

$$h_p^-\leqslant 2^{-\frac{p-3}{2}}p(2^l-1)^{-\frac{p-1}{2l}}\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}$$

$$=2p\left(\frac{p-1}{8(2^l-1)^{2/l}}\right)^{\frac{p-1}{4}}.$$ ∎

系 $h_p^-\leqslant 2p\left(\dfrac{p-1}{31.997158\cdots}\right)^{\frac{p-1}{4}}.$

证明 对于 $2|l$ 情形，由上述引理知道 $h_p^- \leqslant 2p\left(\frac{p-1}{32}\right)^{\frac{p-1}{4}}$. 对于 $2\nmid l$ 情形，如果 $p>127$，易知 $l\geqslant 11$. 而

$$(2^l-1)^{2/l} \geqslant (2^{11}-1)^{2/11} = 3.9996448\cdots,$$

因此

$$h_p^- \leqslant 2p\left(\frac{p-1}{8\times 3.9996448\cdots}\right)^{\frac{p-1}{4}}$$

$$= 2p\left(\frac{p-1}{31.997158\cdots}\right)^{\frac{p-1}{4}}.$$

而对于 $p\leqslant 127$ 用下面表格可以直接验证公式的正确性. ∎

下面是对于 $p\leqslant 127$ 的 h_p^+ 和 h_p^- 值.（如果广义 Riemann 猜想成立，可以证明对于每个素数 $p<163$，均有 $h_p^+=1$. 但是已知 $h_{163}^+=4$.）

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
h_p^+	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
h_p^-	1	1	1	1	1	1	1	3	8	9	37	11^2	211	$5\cdot 139$	4889

p	59	61	67	71	73	79
h_p^+	1	1	1			
h_p^-	$3\cdot 59\cdot 233$	$41\cdot 1861$	$67\cdot 12739$	$7^2\cdot 79241$	$89\cdot 134353$	$5\cdot 53\cdot 377911$

p	83	89	97	101
h_p^-	$3\cdot 279405653$	$113\cdot 118401449$	$577\cdot 3457\cdot 206209$	$5^5\cdot 101\cdot 601\cdot 18701$

p	103	107	109
h_p^-	$5\cdot 103\cdot 1021\cdot 17247691$	$3\cdot 743\cdot 9859\cdot 2886593$	$17\cdot 1009\cdot 9431866153$

p	113	127
h_p^-	$2^3\cdot 17\cdot 11853470598257$	$5\cdot 13\cdot 43\cdot 547\cdot 883\cdot 3079\cdot 626599$

分圆域（及其子域）的类数，类群和单位群结构，以及其他数论性质的研究，一直是代数数论一个富有成果的分支，并且与模形式理论，代数几何（特别是椭圆曲线的算术理论），p-adic 分析，代数

K-理论以及群表示理论交织在一起，构成当前数学研究中极为活跃的边缘性领域．目前关于分圆域的现代理论已有两种好的参考书

[1] S. Lang, Cyclotomic Fields (1978 年)
Cyclotomic Fields II, (1980 年).

[2] L. C. Washington, Introduction to Cyclotomic Fields (1982 年).

我们再介绍一个最基本结果，作为本书的结尾．对于每个素数 $p\geqslant 3$，以 C_{p^n} 表示分圆域 $\mathbb{Q}(\zeta_{p^{n+1}})$ 中唯一的 p^n 次循环子域．对于 $p=2$，以 C_{2^n} 表示 $\mathbb{Q}(\zeta_{2^{n+2}})$ 中唯一的 2^n 次循环子域．现在设 K 是任意代数数域，令 $K_n=Kc_{p^n}$(域的合成)，于是我们有数域的扩张序列：

$$K=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_n\subseteq\cdots$$

记 h_n 为 K_n 的类数，$p^{c(n)}\|h_n$(即 $c(n)$ 是 h_n 元素因子分解式中素因子 p 的指数)．基于和代数几何的类比，岩泽健吉 (Iwasawa) 于 1959 年利用深刻的代数思想证明了如下美妙的公式：存在着与 n 无关的常数 $\mu_p(K)$，$\lambda_p(K)$ 和 $\nu_p(K)$，使得对于每个充分大的 n，均有

$$c(n)=\mu_p(K)p^n+\lambda_p(K)n+\nu_p(K).$$

事实上，岩泽对于更一般的扩张序列证明了类似的结果．岩泽还猜想：对于每个数域 K 和每个素数 p 均有 $\mu_p(K)=0$．1978 年，岩泽的两个学生 Ferrero 和 Washington 对于任意的 Abel 数域证明了这一猜想．但是目前还不清楚这一猜想对于任意数域 K 是否均正确．进而，岩泽和他的另一个学生 Greenberg 猜想，对于每个全实(即 $r_1=[K:\mathbb{Q}]$，$r_2=0$)的数域 K 均有 $\lambda_p(K)=0$．(对于每个素数 p)．不变量 $\lambda_p(K)$ 是很难计算的，对于至今能够计算出 $\lambda_p(K)$ 的全实域 K，均有 $\lambda_p(K)=0$．但是，即使是对于二次域的情形人们也还不知道：对于每个实二次域 K 和每个素数 p，是否均有 $\lambda_p(K)=0$．

习　题

1. 求证:

(a) 如果 χ 为模 m 偶特征, 且 $\chi\neq\chi_0$, 则 $\sum\limits_{k=1}^{m-1}\chi(k)k=0$;

(b) 如果 χ 为模 m 奇特征, 则 $\sum\limits_{k=1}^{m-1}\chi(k)\log\sin\dfrac{k\pi}{m}=0$.

2. 设 K 是分圆域 $\mathbb{Q}(\zeta_p)$ 的子域(p 为奇素数), $n=[K:\mathbb{Q}]$, 求证 $|d(K)|=p^{n-1}$. 又若 K 为虚域, 则 $|d(K_+)|=p^{n/2-1}$.

3. (a) 设 K 是分圆域 $\mathbb{Q}(\zeta_p)$ 的二次子域(p 为奇素数). 则 K 为实二次域 $\Leftrightarrow p\equiv1(\bmod 4)$;

(b) 更一般地, 设 K 是分圆域 $\mathbb{Q}(\zeta_p)$ 的 n 次子域(p 为奇素数). 求证 $p\equiv1(\bmod n)$. 并且: K 为实域 $\Leftrightarrow p\equiv1(\bmod 2n)$.

4. 用二次域的类数解析公式计算 $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{-23})$ 的类数.

5. 在实二次域 K 中, 求证 $V=\prod\limits_{1\leqslant k<|d(K)|/2}\left(\sin\dfrac{k\pi}{|d(K)|}\right)^{\chi_K(k)}$ 是 K 中单位. 进而, 如果以 U_0 表示单位群 $U(K)$ 中由 V 和 -1 生成的乘法子群, 求证: $h(K)=[U(K):U_0]$.

6. 对于虚二次域 $K=\mathbb{Q}(\sqrt{-d})$, $d>3$. $D=|d(K)|$. 求证

(a) $h(K)\leqslant\dfrac{1}{D}\sum\limits_{\substack{1\leqslant k<D/2\\(k,D)=1}}(D-2k)=\dfrac{\varphi(D)}{2}-\dfrac{2}{D}\sum\limits_{\substack{1\leqslant k<D/2\\(k,D)=1}}k$;

(b) 当 $-d\equiv1(\bmod 4)$ 时, $h(K)<d/4$;

当 $-d\equiv2$ 或者 $3(\bmod 4)$ 时, $h(K)<d/2$.

7. 设 p 为奇素数并且 $p\equiv1(\bmod 4)$. $\varepsilon>1$ 为实二次域 $K=\mathbb{Q}(\sqrt{p})$ 的基本单位. 求证

(a) $\eta=\prod\limits_{\substack{0<b<p\\(\frac{b}{p})=-1}}\sin\dfrac{\pi b}{p}\Big/\prod\limits_{\substack{0<a<p\\(\frac{a}{p})=1}}\sin\dfrac{\pi a}{p}$ 为 K 中单位;

(b) $\eta=\varepsilon^{2h(K)}$ 或者 $\eta=\varepsilon^{-2h(K)}$;

(c) $\varepsilon\geqslant\dfrac{1}{2}(1+\sqrt{5})$;

(d) $\prod\limits_{1\leqslant m<p}\sin\dfrac{\pi m}{p}=\dfrac{p}{2^{p-1}}$;

(e) $h(K)<p$.

8. 以 g_s 表示 g^s 模 p 的最小非负剩余, 其中 p 为素数而 g 是模 p 的一个原

据．$m=\dfrac{p-1}{2}$，h_p^- 为分圆域 $\mathbb{Q}(\zeta_p)$ 的类数第一因子．求证：

$$h_p^-=(2p)^{-(m-1)}\left|\det(g_{m+i+j}-g_{i+j})_{0\leqslant i,j\leqslant m-1}\right|.$$

9．计算 h_7^-．

10．证明 $p=37$ 为非正规素数．

附录A　进一步阅读的参考书

不少专家认为，如果想学习代数数论，只需要如下两本书就够了：

[1]　Hecke E., Vorlesungen über die Theorie der algebraishen Zahlen. Leipzig, 1923,（目前已有英译本）.

[2]　Hasse H., Klassenkörper Theorie, Marburg, 1933.

这两本书分别叙述了古典代数数论和类域论中基本而又丰富的数学思想．此后，出现了不少采用局部化方法叙述代数数论的书籍，而且也包括了更多的内容．这方面的书籍有

[3]　Samuel P., Théorie algébrique des nombres, Hermann Paris, 1967.（这是一本美丽的小书，采用纯代数方法，有英译本）.

[4]　Long R. L., Algebraic Number Theory, Marcel-Dekker, 1977.

（本书前言中说："作为一本入门书来说，很难比Samuel"数的代数理论"一书写得更好．本书是打算接着Samuel书的末尾再讲下去"．内容有赋值理论，局部数域的扩张理论和解析理论．最后一章讲数域Galois扩张中群环的作用，是其他书中所没有的．有大量习题和例题.）

[5]　Weiss E., Algebraic Number Theory, McGraw-Hill, 1963.（这是一本很好的入门书）.

[6]　Marcus, D. A., Number Fields, Springer-Verlag, 1977.（有大量例题和习题）.

[7]　Боревич З. И., Шафаревич И. Р., Теория Чисел, «Наука», 1964.（1966年有英译本）（这是以不定方程为中心议题来讲述代数数论．叙述详尽容易阅读．书末有许多数据表）.

[8]　石田信　代數の整數論，1974.（不用局部化方法讲述

代数数论．有大量例题和习题）．

［9］ Artin E., Theory of Algebraic Numbers, Göttingen, 1957.（这是名家著作．有大量例子容易阅读）．

［10］ Hasse H., Zahlentheorie, Academic Verlag, 1949.（有英译本．这是名家巨著．叙述极为详尽）．

［11］ Narkiewitz W., Elementary and analytic Theory of Algebraic Numbers, 华沙，1974.（详尽地叙述了代数数论，书中特别包含许多初等的研究课题．书末有极为丰富的文献目录．）

同时讲解代数数论和类域论的有

［12］ Lang S., Algebraic Number Theory, Addison-Wesley, 1970.

［13］ Janusz G., Algebraic Number Fields, Academic Press, 1973.（是为初学代数数论的人而写．叙述类域论的方式初等而且直接．）

［14］ Goldstein L. J., Analytic Number Theory, Printice-Hall, 1971.（用局部化方法讲代数数论，用解析方法讲类域论）．

［15］ Iyanaga S., The Theory of Numbers, North-Holland, 1975.（全面地介绍了代数数论和类域论．系统地采用上同调方法讲述类域论，书末附有代数数论的详细历史）．

［16］ Weil A., Basic Number Theory, Springer, 1967.（利用富有成效的 Adèle 方法同时处理数域和函数域，采用单代数方法讲述类域论．这本书对于现代数论发展有很大影响）．

讲述类域论的经典文献除了［2］之外还有

［17］ Artin E., Tate J., Class Field Theory, Benjamin, 1968.

专门讲述局部域理论的有两本著名书籍：

［18］ Serre J.-P. Corps locaux, Hermann Paris 1962.（有英译本用代数方法对于局部域的理论作了清晰透彻的阐述．内容丰富．局部类域论的讲述完全而充分地采用了上同调方法）．

［19］ 岩澤健吉　局部類体論　岩波書店 1980 年（是学习局

部类域论的极好入门书．荷兰数学家 Hezewinkel 于 1975 年在文章“Local class field theory is easy”中给出不用上同调群讲述局部类域论的一种新构思．本书将这种思想加以发挥而系统地介绍了局部类域论．中译本已经出版)．

关于代数数论近年来的发展，可见如下两本文集．

[20]　Algebraic Number Theory，由 Cassels J. 和 Fröhlich A. 编，Academic Press，1967．(由名家撰文扼要介绍了代数数论，局部类域论，整体类域论等许多方面的基本内容)

[21]　Algebraic Number Theory，由 Fröhlich A. 编，Academic Press，1977．由名家撰文介绍代数数论当前的研究课题．

关于代数数论方面的文章浩瀚如烟海．1940～1971 年的数论文章均由 LeVeque W. 收集在六卷索引书 Rieview in Number Theory 之中．1972～1985 年的文献，目前也已编辑完毕(同样收在 Rieview in Number Theory 中)．

附录 B 关于群、环、域的一些知识

在这个附录中，我们简要地叙述关于群、环、域的一些基本概念和事实．除了一个例外，我们略去了全部证明．这个例外是：我们在附录的最后给出代数基本定理（复数域的代数封闭性）的一个代数化的证明．

I. 有限生成 Abel 群

设 G 是 Abel（加法）群．如果存在有限个元素 $g_1, \cdots, g_r \in G$，使得 G 中每个元素 g 均可表示成

$$g = n_1 g_1 + \cdots + n_r g_r, \quad n_i \in \mathbb{Z}(\text{整数集合}), \tag{1}$$

则群 G 就叫作是**有限生成的**，而 $g_1, \cdots, g_r$ 叫作是群 G 的**一组生成元素**．G 中有限阶元素 g（即存在 $0 \neq n \in \mathbb{Z}$，使得 $ng = 0$）叫作是**扭元素**．G 中全部扭元素形成一个子群，称作是 G 的**扭子群**，表示成 G_t．如果 $G_t = (0)$，则 G 叫作是**无扭的**．

如果 G 是无扭 Abel 群，并且存在一组有限生成元素 $g_1, \cdots, g_r$，使得 G 中每个元素均可**唯一**地表示成公式(1)的形式，则称 G 是**有限生成的自由 Abel 群**．换句话说，有限生成自由 Abel 群 G 是它的 r 个子群 $\mathbb{Z}g_i = \{ng_i \mid n \in \mathbb{Z}\}\ (1 \leqslant i \leqslant r)$ 的直和：

$$G = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2 \oplus \cdots \oplus \mathbb{Z}g_r.$$

这时，$g_1, \cdots, g_r$ 称作是自由 Abel 群 G 的一组**基**，而 r 叫作是自由 Abel 群 G 的**秩**，表示成 $\operatorname{rank} G$．

(1) （有限生成 Abel 群结构定理）

(a) 若 G 为 n 阶有限 Abel 群，$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是 s 个不同的素数，$\alpha_i \geqslant 1$．则 G 为它的 s 个 Sylow 子群 $G_i\ (1 \leqslant i \leqslant s)$ 的直和：$G = G_1 \oplus \cdots \oplus G_s$，$|G_i| = p_i^{\alpha_i}\ (1 \leqslant i \leqslant s)$．

(b) 每个有限生成 Abel 群 G 均可表示成直和 $G = G_f \oplus G_t$，其中 G_t 是 G 的扭子群（为有限群），而 G_f 是 G 的有限生成自由

Abel 子群.

(c) 有限生成自由 Abel 群 G 的每个子群 H 也是有限生成自由 Abel 群, 并且 $r=\text{rank } H\leqslant \text{rank } G=n$. 进而, 我们可以找到 G 的一组基 $g_1, \cdots, g_n$, 使得

$$G=\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_n, \quad H=\mathbb{Z}d_1g_1\oplus\cdots\oplus\mathbb{Z}d_rg_r,$$

其中 $d_i\neq 0(1\leqslant i\leqslant r)$, 并且 $d_1|d_2|\cdots|d_r$.

II. 环的理想特性和元素特性

本书中的环均指带 1 交换环. 设 S 是环 R 的一个子集合. 定义

$$SR=\{a_1r_1+\cdots+a_nr_n|a_i\in S, r_i\in R, n\geqslant 1\}.$$

这是环 R 的理想, 而且是环 R 中包含集合 S 的最小理想, 称作是**由集合 S 生成的理想**. 如果 $S=\{a_1, \cdots, a_n\}$是 R 的有限子集合, 则 SR 也记作$(a_1, a_2, \cdots, a_n)$, 并且称作是**有限生成的理想**. 特别当 $S=\{a\}$时, $(a)=aR$ 叫作是环 R 的**主理想**. 若环 R 的每个理想都是主理想, 则称 R 为**主理想环**.

设 $I_1, I_2, \cdots, I_n$ 均是环 R 的理想. 定义

$$I_1+I_2+\cdots+I_n=\{a_1+a_2+\cdots+a_n|a_i\in I_i\}.$$

这也是环 R 的理想, 叫作是理想 $I_1, I_2, \cdots, I_n$ 之和. 例如由集合$\{a_1, \cdots, a_n\}$生成的理想即是 $(a_1)+(a_2)+\cdots+(a_n)=a_1R+a_2R+\cdots+a_nR$. 如果 $I_1+I_2=(1)=R$, 则称理想 I_1 和 I_2 **互素**.

环 R 中元素 a 叫作是 R 中的**零因子**, 如果 $a\neq 0$ 并且存在 $0\neq b\in R$, 使得 $ab=0$. 没有零因子的(带 1 交换)环叫作是**整环**. 如果整环 D 同时是主理想环, 则称 D 为**主理想整环**. 每个整环 D 均可嵌在一个域中, 并且具有这样性质的最小域不计同构是唯一决定的, 称作是整环 D 的**商域**.

环 R 中的乘法可逆元叫作是 R 中的**单位**. 环 R 中全部单位形成乘法群, 叫作是环 R 的**单位群**, 表示成 $U(R)$. 当 $|R|\geqslant 2$ 并且 $U(R)=R-\{0\}=R^{\times}$ 时, R 就叫作是**域**.

设 $\mathfrak{p}$ 是环 R 的一个理想. $\mathfrak{p}\neq R$. 称 $\mathfrak{p}$ 是环 R 的**素理想**, 是

指：$ab\in\mathfrak{p}$, a, $b\in R\Rightarrow a\in\mathfrak{p}$ 或者 $b\in\mathfrak{p}$. 称 $\mathfrak{p}$ 是环 R 的极大理想，是指：R 中不存在理想 I，使得 $\mathfrak{p}\subsetneqq I\subsetneqq R$. 我们有：

(2) (a) $\mathfrak{p}$ 为环 R 的素理想 $\Leftrightarrow R/\mathfrak{p}$ 为整环；

(b) $\mathfrak{p}$ 为环 R 的极大理想 $\Leftrightarrow R/\mathfrak{p}$ 为域.

由于域均是整环，从而极大理想均是素理想. 利用 Zorn 引理可以证明：任意(带 1 交换)环中至少存在一个极大理想，从而也至少存在一个素理想.

(3) (中国剩余定理) 设 I_1, I_2, $\cdots$, I_n 是环 R 中两两互素的理想，则有环的自然同构

$$R/I_1\cap I_2\cap\cdots\cap I_n\cong R/I_1\oplus R/I_2\oplus\cdots\oplus R/I_n,$$

$$a\left(\mathrm{mod}\bigcap_{i=1}^{n}I_i\right)\mapsto(a(\mathrm{mod}\,I_1),\ a(\mathrm{mod}\,I_2),\ \cdots,\ a(\mathrm{mod}\,I_n)).$$

设 R 为环. a, $b\in R$, $a\neq 0$. 如果存在 $x\in R$，使得 $ax=b$，我们称 a 整除 b，表示成 $a|b$. 这时 a 叫作是 b 的因子，而 b 叫作是 a 的倍元. 如果不存在满足上述条件的 x，则称 a 不能整除 b，表示成 $a\nmid b$. 设 a, $b\in R^*=R-\{0\}$. 如果 $a|b$ 同时 $b|a$，则元素 a 和 b 叫作是相伴的，表示成 $a\sim b$. 当 R 是整环时，$\sim$ 是 R^* 上的等价关系. 这是因为：$a\sim b\Leftrightarrow a$ 和 b 相差一个单位因子.

假设 a, b, $c\in R^*$, $a=bc$, 并且 b 和 c 均不是 R 中单位(即 b 和 c 均不与 a 相伴)，则 b(和 c)叫作是 a 的真因子. R^* 中元素 a 叫作是环 R 的不可约元素，如果 $a\notin U(R)$ 并且 a 没有真因子. 环 R 中这些元素特性与其理想特性的联系是：

(4) $a|b\Leftrightarrow(b)\subseteq(a)$; $a\sim b\Leftrightarrow(a)=(b)$;

$u\in U(R)\Leftrightarrow u\sim 1_R\Leftrightarrow(u)=R\Leftrightarrow u|r$(对于每个 $r\in R$).

整环 R 叫作是唯一因子分解整环(简记作 UFD)，是指

(i) (分解的存在性) 每个非零非单位元素 $a\in R$ 均可写成 R 中有限个不可约元素之积；

(ii) (分解的唯一性) 如果 $a=c_1\cdots c_n=d_1\cdots d_m$ 是元素 a 的两个分解式，其中 c_i, d_j 均是 R 中的不可约元素，则 $n=m$，并且存在集合 $\{1, 2, \cdots, n\}$ 上的一个置换 σ，使得 $c_i\sim d_{\sigma(i)}$ $(1\leqslant i\leqslant n)$.

(5) 主理想整环均是 UFD. 若 F 为域, 则多项式环 $F[x]$ 是主理想整环, 从而也是 UFD.

(6) (Gauss). 若 R 是 UFD, 则多项式环 $R[x]$ (从而 $R[x_1, x_2, \cdots, x_t]$) 也是 UFD.

设 a 和 b 是环 R 中两个非零元素. $d \in R$ 叫作是 a 和 b 的最大公因子(表示成 (a, b)), 如果: (i) $d|a$ 并且 $d|b$; (ii) 若 $e|a$, $e|b$, $e \in R$, 则 $e|d$. 类似地可以定义 a 和 b 的最小公倍元(表示成 $[a, b]$). 以及多个元素的最大公因子 $(a_1, a_2, \cdots, a_n)$ 和最小公倍元 $[a_1, a_2, \cdots, a_n]$. 如果 $d=(a, b)$, 则与 d 相伴的每个元素均是 a 和 b 的最大公因子. 对于最小公倍元也有类似的结论. 如果 R 是 UFD, 则任意 n 个非零元素 $a_1, \cdots, a_n$ 均有最大公因子和最小公倍元. 而当 R 是主理想整环时, 我们有:

$$(a_1)+(a_2)+\cdots+(a_n)=((a_1, \cdots, a_n))$$

(由元素 $(a_1, \cdots, a_n)$ 生成的主理想),

$$(a_1) \cap (a_2) \cap \cdots \cap (a_n)=([a_1, \cdots, a_n]).$$

(7) (Eisenstein 不可约判别法). 设 D 为 UFD, F 是 D 的商域. $f(x)=\sum_{i=0}^{n} a_i x^i \in D[x]$. $\deg f$ (多项式 $f(x)$ 的次数) $\geqslant 1$. p 是 D 中一个不可约元素. 并且 $p \nmid a_n$, $p | a_i (0 \leqslant i \leqslant n-1)$, $p^2 \nmid a_0$. 则

(a) $f(x)$ 是 $F(x)$ 中的不可约元素. 进而,

(b) 如果在 D 中还有 $(a_0, a_1, \cdots, a_n)=1$, 则 $f(x)$ 也是 $D[x]$ 中的不可约元素.

III. 域的扩张, 域的伽罗华理论

设 K 和 F 均为域. 如果 K 是 F 的子域, 则称 F 是 K 的扩域或(域的)扩张, 并且常常把这样一对域表示成 F/K.

设 F 是域而 X 是 F 的一个子集合. 则 F 中包含 X 的最小子域叫作是 F 中由集合 X 生成的子域. 如果 K 是 F 的子域而 X 是 F 的子集合, 则 F 中由集合 $K \cup X$ 生成的子域也叫作是 X

在域 K 上生成的域，并且表示成 $K(X)$，而由集合 $K\cup X$ 生成的子环表示成 $K[X]$．如果 $X=\{u_1, \cdots, u_n\}$，则 $K(X)$ 和 $K[X]$ 也分别表示成 $K(u_1, \cdots, u_n)$ 和 $K[u_1, \cdots, u_n]$，并且称域 $K(u_1, \cdots, u_n)$ 是 K 的有限生成扩张．特别当 $n=1$ 时，域 $K(u)$ 叫作是域 K 的单扩张．如果 L 和 M 均是域 F 的子域，我们将 F 中由 $L\cup M$ 生成的子域叫作是域 L 和 M 的合成，并且表示成 LM．于是 $LM=L(M)=M(L)=ML$．类似地可以定义多个域的合成．

设 F/K 是域的扩张，则 F 是域 K 上的向量空间．我们以 $[F:K]$ 表示向量空间 F 在 K 上的维数，并且称作是扩张 F/K 的次数．当 $[F:K]$ 有限时，称 F/K 为有限(次)扩张，否则叫作是无限(次)扩张．

(8) 设 F/E 和 E/K 均是域的扩张，则

$$[F:K]=[F:E][E:K].$$

(9) 设 F 为 K 的扩域．$u, u_i\in F, X\subseteq F$．则

(i) $K[u]=\{f(u)\mid f(x)\in K[x]\}$,

$$K[u_1, \cdots, u_m]=\{f(u_1, \cdots, u_m)\mid f(x_1, \cdots, x_n)\in K[x_1, \cdots, x_n]\},$$

$$K(X)=\{f(u_1, \cdots, u_n)\mid f(x_1, \cdots, x_n)\in K[x_1, \cdots, x_n], u_1, \cdots, u_n\in X, n\geqslant 1\};$$

(ii) $K(u)=\{f(u)/g(u)\mid f(x), g(x)\in K[x], g(u)\neq 0\}$,

$$K(u_1, \cdots, u_m)=\{f(u_1, \cdots, u_m)/g(u_1, \cdots, u_m)\mid f(x_1, \cdots, x_m), g(x_1, \cdots, x_m)\in K[x_1, \cdots, x_m], g(u_1, \cdots, u_m)\neq 0\},$$

$$K(X)=\{f(u_1, \cdots, u_n)/g(u_1, \cdots, u_n)\mid f, g\in K[x_1, \cdots, x_n], g(u_1, \cdots, u_n)\neq 0, u_1, \cdots, u_n\in X, n\geqslant 1\};$$

(iii) 对于每个元素 $v\in K[X]$（或 $K(X)$），均有 X 的有限子集合 X'，使得 $v\in K[X']$（或 $K(X')$）．

设 α 为域 F 中元素，$f(x)\in F[x]$．如果 $f(\alpha)=0$，称 α 为多项式 $f(x)$ 的根．根据余数定理，这等价于在多项式环 $F[x]$ 中

$(x-\alpha)|f(x)$. 设m为正整数，使得$(x-\alpha)^m|f(x)$，$(x-\alpha)^{m+1}\nmid f(x)$. m叫作是根α的重数. 当$m\geqslant 2$时，α叫作是$f(x)$的重根. 如果$m=1$，则α叫作是$f(x)$的单根.

对于$f(x)=\sum_{i=0}^{n}c_ix^i\in F[x]$. 我们将多项式

$$f'(x)=\sum_{i=1}^{n}ic_ix^{i-1}\in F[x]$$

叫作是$f(x)$的形式微商.

(10) 设F为域，$f(x)\in F[x]$，$\deg f=n$.

(a) $f(x)$在域F中根的个数(重根按重数计算)至多为n.

(b) $f(x)$在F的某个扩域中有重根$\Leftrightarrow(f,f')\neq 1$.

(c) 如果$f(x)$是$F[x]$中的不可约多项式. 则当F为特征零域时，$f(x)$没有重根；而当F为特征p(p为素数)域时，$f(x)$在F的某个扩域中有重根的充要条件是它为x^p的多项式，即存在$g(x)\in F[x]$，使得$f(x)=g(x^p)$.

设F是K的扩域. 元素$u\in F$叫作是K上的代数元素，是指存在某个非零多项式$f(x)\in F[x]$，使得$f(u)=0$. 反之，如果u不是$K[x]$中任何非零多项式的根，则称u是K上的超越元素. 如果F中每个元素均是K上的代数元素，则称F是K的代数扩张. 反之，如果F中至少有一个元素在K上是超越的，则称F是K的超越扩张.

域K上的多项式环$K[x_1,\cdots,x_n]$是整环. 它的商域$K(x_1,\cdots,x_n)$叫作是域K上关于未定元$x_1,\cdots,x_n$的有理函数域.

(11) 设F为K的扩域，$u\in F$是K上的超越元素. 则

(a) 存在域的同构$\sigma: K(x)\cong K(u)$，使得σ在K上的限制$\sigma|_K$是域K的恒等自同构.

(b) $K(u)/K$是无限(超越)扩张.

(12) 设F为K的扩域，$u\in F$是K上的代数元素. 则

(a) $K(u)=K[u]$；

(b) $K[x]$中存在唯一的不可约首1(即最高项系数是1)的多项式$f(x)\in K[x]$，$(\deg f=n\geqslant 1)$，使得$f(u)=0$，并且

$$K(u)\cong K[x]/(f(x)).$$

(c) $[K(u):K]=n$, 并且$\{1, u, u^2, \cdots, u^{n-1}\}$是向量空间$K(u)$的一组 K-基.

(d) $K(u)/K$ 是(有限)代数扩张.

注记 (a) (12)中所述的多项式$f(x)$叫作是代数元素u在域K上的极小多项式. 这是因为它有如下的性质: (i) $f(u)=0$; (ii) $g(x)\in K[x]$, $g(\alpha)=0\Rightarrow f(x)\mid g(x)$.

(b) 令$\deg f=n=[K(u):K]$. 我们也称u是K上的n次代数元素. (12)表明: 这时域$K(u)$中每个元素均可唯一地表示成如下形式: $a_0+a_1u+\cdots+a_{n-1}u^{n-1}$, $a_i\in K$.

(13) 设K为域, $f(x)$是$K[x]$中任一多项式, $\deg f\geqslant1$, 则存在K的单扩张$F=K(u)$, 使得$f(u)=0$. 进而, 如果$f(x)$是$K[x]$中的不可约多项式, 并且$F_1=K(u_1)$是K的另一个单扩张, 使得$f(u_1)=0$, 则存在域的同构$\sigma: F\xrightarrow{\sim}F_1$, 使得$\sigma(u)=u_1$, 并且$\sigma|_K$是域$K$的恒等自同构.

注记 我们将(13)中的域$K(u)$称作是将$f(x)$的根u添加到K上而得到的域. 如果作多次的添加, 我们就可找到K的某个扩域M, 使得$f(x)$的全部根都在M中, 即$f(x)$在$M[x]$中分解成一些一次多项式的乘积. K的满足这种性质的最小扩域叫作是$f(x)$在K上的分裂域. 换句话说, 域M叫作是多项式$f(x)\in K[x]$在K上的分裂域, 是指:

(i) $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(\alpha-\alpha_n)$, $\alpha_i\in M$, $n=\deg f$;

(ii) $F=K(\alpha_1, \alpha_2, \cdots, \alpha_n)$,

$f(x)$在K上的任意两个分裂域是彼此同构的.

设K是域. 如果每个在K上代数的元素均属于K, 则称K是代数封闭域. 例如, 我们在本附录的最后要证明复数域$\mathbb{C}$是代数封闭域. 对于任意域K, 设Ω是将在K上代数的全部元素添加到K上而得到的域, 则Ω是代数封闭域, Ω叫作是域K的代数闭包. Ω的代数封闭性是基于:

(14) (a) 若u是F上的代数元素而F/K是域的代数扩张,

则 u 也是 K 上的代数元素.

(b) 若 F/M, M/K 均是域的代数扩张, 则 F/K 也是代数扩张.

有理数域 $\mathbb{Q}$ 的有限(次)扩域(从而是代数扩张)K 叫作是**代数数域**, 简称作**数域**. 这是代数数论的基本研究对象. 由于复数域 $\mathbb{C}$ 是 $\mathbb{Q}$ 的代数封闭扩域, 我们可以将所有的数域均看成是 $\mathbb{C}$ 的子域. 现在叙述数域的伽罗华扩张理论.

数域 K 到 $\mathbb{C}$ 中的每个单同态也叫作是 K 到 $\mathbb{C}$ 中的**嵌入**. 设 L/K 是数域的扩张, σ: $L\to\mathbb{C}$ 为嵌入. 如果 $\sigma(K)=K$ 并且 $\sigma|_K$ 是域 K 的恒等自同构, 则称 σ 为 L 到 $\mathbb{C}$ 中的一个 **K-嵌入**. 类似地, 设 L_1/K, L_2/K 均是数域的扩张. 如果 σ: $L_1\cong L_2$ 是域同构并且 $\sigma|_K$ 是域 K 的恒等自同构, 则称 σ 是 **K-同构**, 特别当 $L_1=L_2=L$ 时, 则称 σ 为 L 的 **K-自同构**. L 的全部 K-自同构全体显然形成群, 叫作是扩张 L/K 的**伽罗华群**, 表示成 $\mathrm{Gal}(L/K)$. (注意对于 σ, $\tau\in\mathrm{Gal}(L/K)$, 定义 $\sigma\tau$ 为: $\sigma\tau(a)=\sigma(\tau(a))$, $a\in L$). 可以证明 $|\mathrm{Gal}|(L/K)|\leqslant[L:K]$.

设 L/K 是数域的扩张. σ: $L\to\mathbb{C}$ 为一个 K-嵌入. 对于 $a\in L$, $\sigma(a)\in\mathbb{C}$ 叫作是元素 a 的 **K-共轭元素**. 设 $f(x)\in K[x]$ 是元素 a 在 K 上的极小多项式, 则 $f(x)$ 在 $\mathbb{C}$ 中的全部根恰好是 a 的全部 K-共轭元素. 类似地, $\sigma(L)$ 叫作是域 L 的 **K-共轭域**.

数域扩张 L/K 叫作是**伽罗华扩张**(或叫**正规扩张**), 如果 L 是 K-自共轭域. 也就是说, 如果对于每个 K-嵌入 σ: $L\to\mathbb{C}$, 均有 $\sigma(L)=L$.

(15) 设 L/K 是数域的扩张. 则以下几条彼此等价

(a) L/K 是伽罗华扩张;

(b) 对于 L 中每个元素 a 和每个 K-嵌入 σ: $L\to\mathbb{C}$, 均有 $\sigma(a)\in L$;

(c) L 是某个多项式 $f(x)\in K[x]$ 在 K 上的分裂域;

(d) $|\mathrm{Gal}(L/K)|=[L:K]$.

设 F/K 是数域的伽罗华扩张. 则对于 F/K 的每个中间域

M, $K\subseteq M\subseteq F$, F/M 也是伽罗华扩张, 并且 $\mathrm{Gal}(F/M)$ 是 $\mathrm{Gal}(F/K)$ 的子群. 另一方面, 对于 $\mathrm{Gal}(F/K)$ 的每个子群 H, 令

$$\mathrm{Fix}(H)=\{a\in F\mid \sigma(a)=a,\ \forall\sigma\in H\},$$

这是 F/K 的中间域, 叫作是 F 的 H-固定子域.

(16) (伽罗华扩张基本定理). 设 F/K 是数域的伽罗华扩张. 以 $\mathfrak{M}$ 表示 F/K 的全部中间域所组成的集合, 以 $\mathfrak{G}$ 表示 $\mathrm{Gal}(F/K)$ 的全部子群组成的集合. 定义映射

$$\varphi:\mathfrak{M}\to\mathfrak{G},\quad \varphi(M)=\mathrm{Gal}(F/M);$$

$$\psi:\mathfrak{G}\to\mathfrak{M},\quad \psi(H)=\mathrm{Fix}(H).$$

则

(a) 对于每个 $M\in\mathfrak{M}$, $\psi\varphi(M)=M$; 对于每个

$$H\in\mathfrak{G},\quad \varphi\psi(H)=H.$$

从而 φ 和 ψ 给出集合 $\mathfrak{M}$ 与 $\mathfrak{G}$ 之间的一一对应, 并且 $\varphi=\psi^{-1}$.

(b) 设 H_1, $H_2\in\mathfrak{G}$, M_1, $M_2\in\mathfrak{M}$. 则

$$H_1\supseteq H_2\Leftrightarrow\psi(H_1)\subseteq\psi(H_2);$$

$$M_1\supseteq M_2\Leftrightarrow\varphi(M_1)\subseteq\varphi(M_2).$$

$$\varphi(M_1\cap M_2)=\text{由 }\varphi(M_1)\text{ 和 }\varphi(M_2)\text{ 生成的群},$$

$$\varphi(M_1M_2)=\varphi(M_1)\cap\varphi(M_2).$$

(c) 设 $M\in\mathfrak{M}$. 则 M/K 为伽罗华扩张 $\Leftrightarrow\varphi(M)=\mathrm{Gal}(F/M)$ 是 $\mathrm{Gal}(F/K)$ 的正规子群. 并且在这个时候,

$$\mathrm{Gal}(M/K)\cong\mathrm{Gal}(F/K)/\mathrm{Gal}(F/M).$$

IV. 有限域

(17) (a) 每个有限域 F 均是 p^n 元域, 其中 $n\geqslant1$, p 为素数并且 p 是域 F 的特征. F 有一个 p 元子域 $\mathbb{F}_p$, 并且 $F/\mathbb{F}_p$ 是 n 次扩张.

(b) p^n 元域 F 的加法群是 n 个 p 阶循环群的直和. 而 $F^*=F-\{0\}$ 是 p^n-1 阶乘法循环群. 设 u 是乘法循环群 F^* 的一个生成元, 则 $F=\{0,1,u,u^2,\cdots,u^{p^n-2}\}=\mathbb{F}_p(u)$, 从而 $F/\mathbb{F}_p$ 是单扩张.

(c) 固定 $\mathbb{F}_p$ 的一个代数闭包 Ω_p 并且设 $F\subseteq\Omega_p$. 则 p^n 元域 F 即是多项式 $x^{p^n}-x\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p$ 上的分裂域. 因此对于每个正整数 n, Ω_p 中均存在唯一的 p^n 元子域.

(d) 阶数相同的两个有限域彼此同构.

(e) 设 F 为 p^n 元域,则映射 σ_p: $F\to F$, $\sigma_p(\alpha)=\alpha^p(\alpha\in F)$是域 F 的 n 阶自同构, 称作是域 F 的 Frobenius 自同构. 并且 F 的自同构群 $\mathrm{Aut}(F)$ 即是由 σ_p 生成的 p 阶循环群.

(f) 我们以$\mathbb{F}_q$ 表示 q 元域(它不计同构是唯一的). 设 $\mathbb{F}_{p^m}, \mathbb{F}_{p^n}\subset\Omega_p$. 则 $\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}\Leftrightarrow m|n$. 并且在这个时候, $\mathbb{F}_{p^n}$ 的 $\mathbb{F}_{p^m}$-自同构群 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})=\{\sigma\in\mathrm{Aut}\mathbb{F}_{p^n}\,|\,\sigma(\alpha)=\alpha$, 对每个 $\alpha\in\mathbb{F}_{p^m}\}$是由 σ_p^m 生成的 n/m 阶循环群. 我们将 σ_p^m: $\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, $\sigma_p^m(\alpha)=\alpha^{p^m}(\alpha\in\mathbb{F}_{p^n})$ 称作是扩张 $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ 的 Frobenius 自同构. 另一方面, 对于 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)=\langle\sigma_p\,|\,\sigma_p^n=1\rangle$中唯一的 n/m 阶循环子群$\langle\sigma_p^m\rangle$, 它的固定子域恰好是 $\mathbb{F}_{p^m}$, 即 $\mathbb{F}_{p^m}=\{\alpha\in\mathbb{F}_{p^n}\,|\,\sigma_p^m(\alpha)=\alpha\}$.

V. 代数基本定理

(18) 复数域 $\mathbb{C}$ 是代数封闭域.

这相当于说: 每个复系数多项式 $f(x)$ $(\deg f(x)=n\geqslant1)$ 必有复根. 并且熟知它也等价于: n 次复系数多项式恰好有 n 个复根(计算重数).

有人统计,代数基本定理共有近两百个证明. 更有趣的是,所有的证明都要利用数学分析中的某些事实. 我们这里所介绍的一个证明也不例外. 因为我们要利用

引理 1 每个奇次实系数多项式必有实根.

大家知道,这一事实从连续函数的中值定理得出,此外我们还需要(与数学分析无关的)

引理 2 复系数 2 次多项式的根均是复根.

证明 设 $f(x)$是复系数 2 次多项式. 不妨设它是首 1 的, 即 $f(x)=x^2+\alpha x+\beta$, α, $\beta\in\mathbb{C}$. 由于 $f(x)=\left(x+\frac{\alpha}{2}\right)^2+\beta-\frac{\alpha^2}{4}$,

我们只需证明每个多项式 $g(z)=z^2-\gamma(\gamma\in\mathbb{C})$ 的根均是复根即可. 令 $\gamma=a+bi$, a, $b\in\mathbb{R}$. 取

$$z_0,\ z_1=\begin{cases}\pm\left(\sqrt{\dfrac{\sqrt{a^2+b^2}+a}{2}}+i\sqrt{\dfrac{\sqrt{a^2+b^2}-a}{2}}\right), & 若\ b\geqslant 0.\\ \pm\left(\sqrt{\dfrac{\sqrt{a^2+b^2}+a}{2}}-i\sqrt{\dfrac{\sqrt{a^2+b^2}-a}{2}}\right), & 若\ b<0.\end{cases}$$

直接验证即知 z_0 和 z_1 是 $g(z)=z^2-\gamma$ 的两个复根. ▌

引理3 每个次数$\geqslant 1$的实系数多项式 $g(x)$ 必有复根.

证明 设 $g(x)\in\mathbb{R}[x]$, $\deg g(x)=d\geqslant 1$. 令 $d=2^n q$, $2\nmid q$, $n\geqslant 0$. 我们对 n 作数学归纳法. 如果 $n=0$, 则 $g(x)$ 为奇次实系数多项式. 由引理1可知它有复根. 下设 $n=n_0\geqslant 1$, 并且对于 n 比 n_0 小的情形引理3成立. 令 x_1, $\cdots$, x_d 为 $g(x)$ 在 $\mathbb{R}$ 的适当的扩域中的全部根. 我们的目的是证明必有某个 $x_i\in\mathbb{C}$.

为证此, 取任意一个实数 c. 令

$$y_{ij}=x_i+x_j+cx_ix_j\quad(1\leqslant i\leqslant j\leqslant d).$$

一共有 $\frac{1}{2}d(d+1)=2^{n-1}q(d+1)$ 个 y_{ij}. 又令

$$\begin{aligned}G(x)&=\prod_{1\leqslant i\leqslant j\leqslant d}(x-y_{ij})\\&=x^m+g_1(x_1,\ \cdots,\ x_d)x^{m-1}+\cdots+g_m(x_1,\ \cdots,\ x_d),\\&\qquad m=2^{n-1}q(d+1).\end{aligned}$$

不难看出, 每个 $g_i(x_1,\ \cdots,\ x_d)$ 均是 x_1, $\cdots$, x_d 的实系数对称多项式, 从而 $g_i(x_1,\ \cdots,\ x_d)\in\mathbb{R}[\sigma_1,\ \cdots,\ \sigma_d]$, 其中 σ_1, $\cdots$, σ_d 为 $x_1,\cdots,x_d$ 的初等对称多项式. 但是 $g(x)=x^d-\sigma_1x^{d-1}+\sigma_2x^{d-2}-\cdots+(-1)^d\sigma_d\in\mathbb{R}[x]$, 从而 σ_1, $\cdots$, $\sigma_d\in\mathbb{R}$. 于是 $g_i(x_1,\ \cdots,\ x_d)\in\mathbb{R}$ $(1\leqslant i\leqslant m)$. 从而 $G(x)\in\mathbb{R}[x]$. 由于 $n\geqslant 1$, 从而 $2|d=2^nq$, 于是 $2\nmid(d+1)q$ 而 $\deg G(x)=2^{n-1}q(d+1)$. 由归纳假设便知 $G(x)$ 有复根 z_c. 换句话说, 我们有 $i(c)$ 和 $j(c)$ (均与 c 有关), 使得

$$y_{i(c),j(c)}=x_{i(c)}+x_{j(c)}+cx_{i(c)}x_{j(c)}=z_c\in\mathbb{C}.$$

由于指标集合 $\{(i,\ j)\}$ 是有限的, 而实数 c 可任意选取, 从而必然有 $c\neq c'$, c, $c'\in\mathbb{R}$, 使得 $i(c)=i(c')$, $j(c)=j(c')$. 令它们分别为

r 和 s, 于是得到

$$x_r+x_s+cx_rx_s=z_c\in\mathbb{C},\qquad x_r+x_s+c'x_rx_s=z_{c'}\in\mathbb{C}.$$

由此及 $c\neq c'$, c, $c'\in\mathbb{R}$ 可知 $x_r+x_s\in\mathbb{C}$, $x_rx_s\in\mathbb{C}$. 于是 $h(x)=x^2-(x_r+x_s)x+x_rx_s\in\mathbb{C}[x]$. 根据引理 2, $h(x)$ 的两个根 x_r 和 x_s 均是复根, 这就证明了存在某个 $i(1\leqslant i\leqslant d)$, 使得 $x_i\in\mathbb{C}$. ▌

最后我们来证代数基本定理: 设 $f(x)=\sum_{i=0}^{n}c_ix^i\in\mathbb{C}[x]$, $\deg f\geqslant 1$. 记 $\bar{f}(x)=\sum_{i=0}^{n}\bar{c}_ix^i$, 其中 $\bar{c}_i$ 表示 c_i 的共轭复数. 令 $g(x)=f(x)\bar{f}(x)$, 易知 $g(x)\in\mathbb{R}[x]$. 根据引理 3, 存在 $\alpha\in\mathbb{C}$ 使得 $g(\alpha)=0$. 于是 α 为 $f(x)$ 或者 $\bar{f}(x)$ 的根. 如果 $f(\alpha)=0$ 则证毕; 如果 $\bar{f}(\alpha)=0$, 则复数 $\bar{\alpha}$ 就是 $f(x)$ 的根. 这就证明了代数基本定理. ▌